※As of June 2021

16 Guideline for Supervision of Crypto-Asset Exchange Service Providers（Provisional Translation）

I. General

I-1 Scope of Crypto-Assets, etc.

I-1-1 Scope of Crypto-Assets and Judgment Criteria for the Applicability

When there is an inquiry, etc. about the applicability of Crypto-Assets as prescribed in Article 2(5) of the Payment Services Act (Act No. 59 of 2009; hereinafter referred to as "the Act"), the supervisory authorities shall make a judgment in light of the definition of Crypto-Assets as prescribed in each item of the same paragraph, while giving consideration to the following points.

It should be noted that, since information and communication technology (ICT) is advancing rapidly and changes day by day, the applicability, etc. of Crypto-Assets shall be ultimately determined individually and specifically, depending on the usage patterns, etc.

Note: It should be noted that even when a financial instrument satisfies all the provisions in each item of Article 2(5) of the Act, it does not fall under the category of Crypto-Assets if it indicates the right to transfer electronic records as prescribed in Article 2(3) of the Financial Instruments and Exchange Act (Act No. 25 of 1948) .

(i) With respect to the applicability of Crypto-Assets as prescribed in Article 2(5)(i) of the Act (hereinafter referred to as "Item (i) Crypto-Assets"), when determining whether a would-be Crypto-Asset "can be used in relation to unspecified persons for the purpose of paying consideration," the supervisory authorities shall request the applicant to explain in detail, for example, about the following: "Does the would-be Crypto-Asset have a mechanism to be transferred among unspecified persons through a network such as a blockchain?" "Whether the contract between the issuer and the store, etc. limits stores, etc. where the Crypto-Asset can be used for payment of consideration" "Whether the issuer manages the stores, etc. where the Crypto-Asset can be used" and so on.

(ii) With respect to the applicability of Item (i) Crypto-Assets, when determining whether a would-be Crypto-Asset "can be purchased from and sold to unspecified persons acting as counterparties," the supervisory authorities shall request the applicant to explain in detail, for example, about the following: "Does the would-be Crypto-Asset have a mechanism to be transferred among unspecified persons through a network such as a blockchain?" "Can it be exchanged for the Japanese currency or a foreign currency without any restriction by the issuer?" "Does it have an exchange market for the Japanese currency or a foreign currency?" and so on.

Note: The so-called "prepaid cards" issued by issuers of Prepaid Payment Instruments and the "Points" in point services (services that issue points according to a certain percentage of the sales amount of goods and services, and services that issue a certain amount of points for each visit and use, etc.) do not satisfy (i) or (ii) above in the relation between these issuers and stores, etc., and do not fall under the category of Crypto-Assets.

(iii) With respect to the applicability of Crypto-Assets as stipulated in Article 2(5)(ii) of the Act, when determining whether a would-be Crypto-Asset "can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties," the supervisory authorities shall request the applicant to explain in detail, for example, about the following: "Does the would-be Crypto-Asset have a mechanism to be transferred among unspecified persons through a network such as a blockchain?" "Is the exchange with Item (i) Crypto-Assets possible without any restriction by the issuer?" "Is there an exchange market

for Item (i) Crypto-Assets?" "Do they have not only the goods and rights, etc. that can be purchased or sold by using Item (i) Crypto-Assets but also any economic functions that are equivalent to those of said Crypto-Assets?" and so on.

(iv) With respect to the applicability of Currency-Denominated Assets that are stipulated in Article 2(6) of the Act, when determining whether their functions enable "performance of obligations, refund, or anything equivalent thereto supposed to be made in the Japanese currency or a foreign currency," the supervisory authorities shall request the applicant to explain in detail about "whether the issuer and its related person(s) (hereinafter referred to as "issuer et al.") have obligations such as being required to provide a refund to a user in legal tender in accordance with a contract, etc. between the issuer et al. and the user."

Note: In cases where a would-be Crypto-Asset falls under the category of Currency-Denominated Assets, despite not falling under that of Crypto-Assets as prescribed in Article 2(5) of the Act, it should be noted that, depending on the contents of said asset and details of the service provider's transactions, it may fall under the category of Prepaid Payment Instruments or exchange transactions, or certain other provisions of laws and regulations.

I-1-2 Applicability of the Crypto-Asset Exchange Services and Judgment Criteria for Appropriateness of Crypto-Assets Handled

I-1-2-1 Purpose and Significance

Information and communication technology (ICT) is advancing rapidly, and various types of Crypto-Assets are assumed to appear every day. In addition, with regard to the form of transactions pertaining to the Crypto-Asset Exchange Services (transactions pertaining to the acts prescribed in each item of Article 2(7) of the Act; the same applies hereinafter), various types are conceivable. Therefore, even if the instrument to be handled falls under the category of Crypto-Assets or the handling of the Crypto-Assets formally falls under transactions pertaining to the Crypto-Asset Exchange Services, there may be cases in which it is not necessarily appropriate for Crypto-Asset Exchange Service Providers to handle the instrument, from the viewpoint of the user protection or public interest. From this perspective, Article 23(1)(v) of the Cabinet Office Order on Crypto-Asset Exchange Service Providers (Cabinet Office Order No. 7 of 2017; hereinafter referred to as "the Cabinet Office Order") requires Crypto-Asset Exchange Service Providers to take necessary measures so that they do not handle Crypto-Assets which are found to be likely to hinder the protection of users or the proper and secure conduct of the Crypto-Asset Exchange Services.

Accordingly, the supervisors shall request applicants to provide detailed explanations on the appropriateness of transactions pertaining to the Crypto-Asset Exchange Services and the appropriateness of Crypto-Assets handled thereby, etc., and shall conduct examination, etc. of applications for registration, in collaboration with each Certified Association for Payment Service Providers (hereinafter collectively referred to as "the Association") as necessary.

I-1-2-2 Judgment Criteria for the Applicability of the Crypto-Asset Exchange Services

When there is an inquiry, etc. about the applicability of the Crypto-Asset Exchange Services as prescribed in Article 2(7) of the Act, the supervisory authorities shall make a judgment in light of the definition of the Crypto-Asset Exchange Services as prescribed in each item of the same paragraph, while giving consideration to the following points.

(i) The phrase "in the course of trade" as stipulated in Article 2(7) of the Act can be understood to mean an act with "vis-a-vis public nature" which is carried out in the form of "repeated

continuity." However, whether a specific act involves "vis-a-vis public nature" or "repeated continuity" should be substantively determined for each individual case in light of the actual situation. With regard to "vis-a-vis public nature" and "repeated continuity," it should be noted that such acts include not only cases where acts with "vis-a-vis public nature" are performed repeatedly and continuously, but also cases where "vis-a-vis public nature" and "repeated continuity" are assumed.

(ii) If any of the following acts is performed for a third party in connection with a contract concerning purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset, the act falls, in principle, under the category of "intermediary for the act set forth in the preceding item." (hereinafter referred to as "Intermediary for Crypto-Asset Transactions") as set forth in Article 2(7)(ii) of the Act.

(A) Solicitation to conclude a contract

(B) Product explanation for the purpose of solicitation to conclude a contract

(C) Negotiation of terms for concluding a contract

Note 1: Whether or not the act is an intermediary needs to be substantively determined for each individual case in light of the actual situation. For example, it should be noted that, even in the case where a display on the Internet is used, if the display can be deemed to be followed by a solicitation action toward the conclusion of a contract with a third party, a series of actions including the display on the Internet can constitute an intermediary.

Note 2: However, if only a part of the administrative processing of the following acts is carried out in connection with purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset, it may be considered an act that does not constitute the Intermediary for Crypto-Asset Transactions.

- Simple distribution and delivery of advertising leaflets, brochures, contract application forms, etc. (including those by electromagnetic means). However, if an explanation is given on how to fill in the document distributed or delivered, beyond simple distribution or delivery, such act may fall under the category of Intermediary for Crypto-Asset Transactions.
- Receipt and collection of contract application forms and attached documents. However, if the content of a filled-in contract application form is checked, beyond the simple receipt and collection of the contract application form or beyond pointing out any wrong description or omission in the contract application form or failure to attach at least one of the necessary documents, the act may fall under the category of Intermediary for Crypto-Asset Transactions.
- Explanations given in seminars, etc. about the structures and how to utilize general Crypto-Assets.

(iii) Whether or not an act falls under the category of "management of Crypto-Assets on behalf of another person" as provided for in Article 2(7)(iv) of the Act should be substantively determined for each individual case in light of the actual situation. However, in a case where the business operator is in a state in which the business operator is able to proactively transfer a Crypto-Asset of a user, such as a case where the business operator holds a secret key sufficient to enable the business operator to transfer the Crypto-Asset of the user without any involvement of the user, either alone or in cooperation of an affiliated business operator, such a case falls under the management of Crypto-Assets as provided for in the same Item.

Note: The borrowing of Crypto-Assets prescribed in Article 23(1)(viii) of the Cabinet Office

Order does not fall under the management of Crypto-Assets prescribed in Article 2(7)(iv) of the Act, but falls under the management of Crypto-Assets prescribed in the same Item, if a business operator substantially manages a Crypto-Asset on behalf of another person under the name of the borrowing of a Crypto-Asset such that the user can receive the return of the Crypto-Asset borrowed at any time at the request of the user.

(iv) If a business operator engaged in Exchange of Crypto-Assets, etc. undergoes or undertakes and carries out the transfer of money upon receiving a request to the effect that money shall be transferred, the business operator may be required to register as a Funds Transfer Service Provider under Article 37 of the Act as an entity engaged in exchange transactions.

(v) With respect to transactions such as futures transactions using Crypto-Assets, there are two types of trading: one involves delivery in kind of the Crypto-Asset which is the purpose of the trading, at the time of settlement, while the other type of trading (hereinafter referred to as "net settlement trading") can be settled only by transferring money or another Crypto-Asset which is the means of settlement in the trading, without delivery in kind of the Crypto-Asset which is the purpose of the trading, by conducting reversing trading, etc. If either type of trading falls under the Derivatives Transactions as defined in Article 2(20) of the Financial Instruments and Exchange Act, it shall be subject to the regulations of the Financial Instruments and Exchange Act. Therefore, registration of the Crypto-Asset Exchange Services is not required unless it involves management of users' Crypto-Assets. Accordingly, when determining whether or not a transaction requires registration of the Crypto-Asset Exchange Services, the supervisors needs to individually and specifically check details of each transaction.

I-1-2-3 Judgment Criteria for the Appropriateness of Crypto-Assets Handled

When examining an application for registration and determining the appropriateness of a Crypto-Asset handled by a Crypto-Asset Exchange Service Provider, the supervisory authorities shall request a detailed explanation from the applicant and the Crypto-Asset Exchange Service Provider, regarding the structures of the Crypto-Asset (including the issuer, the administrator, and other related person(s), as well as details of any project closely related to the Crypto-Asset, etc.), the assumed use(s), the distribution situation, and the technology applied to the Crypto-Asset, as well as regarding details of risks that may arise from the handling of the Crypto-Asset, including risks used for terrorist financing, money laundering, and other purposes, IT system risks, etc., in light of how the internal readiness for handling the Crypto-Asset is ensured. In addition, the supervisory authorities shall decide whether it is appropriate for the Crypto-Asset Exchange Service Provider to handle the Crypto-Asset, from the viewpoint of protecting users and ensuring the proper and secure conduct of business, based on complaints from users and external information such as the Association's opinion.

Note 1: In particular, it should be noted that the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Handling Crypto-Assets" stipulate that the appropriateness of handling Crypto-Assets must be carefully judged when they are (i) likely to be used in a manner that violates laws and regulations or public order and morals, (ii) likely to be used for crimes, and/or (iii) likely to be used for terrorist financing or money laundering, etc. In addition, it should be noted that the same rules prohibit the handling of Crypto-Assets falling under any of the following categories, in light of the characteristics of Crypto-Assets and the preparedness of Crypto-Asset Exchange Service Providers. The rules also state that Crypto-Assets, for which the tracking of transfer records is extremely difficult, should not be

handled unless these problems are resolved, because there is a high risk of them being used for terrorist financing and money laundering, etc., and because it may not be possible to conduct appropriate audits.

- Those that are found to have serious problems or concerns with updating or maintaining the transfer or retention records.
- Those that are difficult to be audited by any certified public accountant or audit corporation
- Those that are difficult to securely store and collect in the relevant system.
- Other than the above, those that involve difficulty in properly and reliably performing the obligations under the Payment Services Act.

Note 2: For example, when offering for sale of a newly issued Crypto-Asset, even if the liquidity is lacking at the stage of issuance, a comprehensive judgment shall be made by fully considering the explanation from the applicant and external information, rather than immediately judging that handling of the Crypto-Asset is inappropriate.

II. Supervisory Viewpoints of Crypto-Asset Exchange Service Providers

II-1 Business Management, etc.

II-1-1 Purpose and Significance

Given that Crypto-Asset Exchange Service Providers manage users' property due to the nature of their business, and that Crypto-Assets are at high risk of being used for terrorist financing and money laundering, etc., it is necessary to take appropriate measures to protect users, such as separate management of users' money and Crypto-Assets, as well as countermeasures against terrorist financing and money laundering.

Moreover, in order to maintain and improve business operation frameworks, it is important to ensure that management discipline functions effectively and that business management is conducted appropriately.

When supervising Crypto-Asset Exchange Service Providers, the following points, for example, shall be taken into consideration. In supervising them, it is necessary to pay attention to the changes in the environment surrounding the Crypto-Asset Exchange Services, to respect the autonomy of Crypto-Assets Exchange Service Providers, to pay attention to the lack of specialized regulations for Crypto-Assets Exchange Service Providers and that there are various business types and scales, and to take actions based on the actual conditions, including changes in the business operations and characteristics of the Crypto-Assets Exchange Service Providers.

II-1-2 Major Supervisory Viewpoints

(i) Does the management team clearly define business policies based on the overall picture at which Crypto-Asset Exchange Service Providers should aim? Then, does the management team draw up clear-cut business plans in line with the established business policies and familiarize all personnel in the firm with those plans? Is the progress of each business plan reviewed periodically and revised whenever necessary?

(ii) Does the management team identify and evaluate management risks that may arise from conducting operations, after taking into account the business model, business details, the scale of its business, conditions of its overseas bases, and the characteristics of Crypto-Assets handled? Also, are the methods of responding to the identified and evaluated management risks reflected in the business plan and the business management?

Note: In identifying and evaluating management risks, it should be noted that the management must have a framework to analyze various risks that have been detected in each department (Sales Department, Internal Control Department, Internal Audit Department). (In the case where there are overseas bases, the relationship with those overseas bases should be taken into account.)

(iii) Do directors warn against and deter dogmatic actions by the representative directors or other top executives? Are directors actively involved in the Board of Directors' processes to make decisions for business execution and to oversee directors' business execution?

(iv) Does the management team not only observe the financial basis prescribed in Article 9(1) of the Cabinet Office Order, but also strive to secure a financial basis appropriate to the business operations and characteristics? Based on the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Financial Management Pertaining to the Crypto-Asset Exchange Services," has the management team established financial risk management frameworks in light of the business model, business details, the scale of its business, conditions of its overseas bases, and the characteristics of Crypto-Assets handled? For example, does it analyze and identify market risks, counterparty risks, and other financial risks, as well as operational risks (including the risk of leakage of Crypto-Assets) and then establish methods for managing such risks?

Note 1: When examining the financial risk management framework, it should be noted that the aforementioned self-regulatory rules require the identification of such risks, the development of management environments, and the preparation and implementation of management plans to maintain and improve financial soundness.

Note 2: When depositing money or a Crypto-Asset to a counterparty of a cover transaction, it is necessary to perform credit screening/management of the counterparty as part of financial risk management. In addition, it is necessary to confirm whether the counterparty appropriately controls the Crypto-Asset so that it does not leak out.

(v) Does the management team have an internal control environment in place for the appropriate and timely disclosure of financial information and other corporate information in accordance with Article 23(1)(vii) of the Cabinet Office Order and the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Financial Management Pertaining to the Crypto-Asset Exchange Services"?

(vi) When managing Crypto-Assets, does the management team select an appropriate certified public accountant or audit corporation for conducting the audit of financial statements and audit of separate management, in consideration of the business details, the scale of its business, characteristics of Crypto-Assets handled, etc.?

(vii) With full awareness that Crypto-Asset Exchange Service Providers are required to protect users and ensure the proper and secure conduct of operations in accordance with law, does the management team, in order to ensure not only business performance such as business promotion and profit expansion, but also compliance with laws and regulations and proper business operations, regard matters related to the establishment and development of internal control environments (including the securing of necessary human and physical resources) as one of the most important management issues, such as the strengthening of the functions of the Internal Control Department and the Internal Audit Department, and take sincere and proactive measures to formulate and disseminate specific policies for the implementation thereof?

Note: The term "Internal Control Department" as used in these Guidelines refers to the

divisions in charge of management of internal affairs, the legal division, etc. for ensuring business operations in compliance with laws and regulations as well as internal rules, etc. In addition, the term "Internal Audit Department" refers to the divisions in charge of inspection, the divisions in charge of auditing, etc. independent from the sales departments, and does not include inspections, etc. conducted by the departments, etc. that are subject to audit as part of internal control.

(viii) With regard to monitoring, etc. according to the authority of the sales manager, does the management team have frameworks in place to conduct monitoring/verification and formulate improvement measures, which are designed to ensure appropriate business operations for divisions in which the Internal Control Department deals with users?

(ix) Does the management team recognize the importance of internal audits concerning transactions related to the Crypto-Asset Exchange Services, and appropriately set the objectives of internal audits? In addition, has the management team established an environment in which the Internal Audit Department can fully exercise its functions? In addition, does the management team approve basic matters described in internal audit plans including audit policies and priority issues, only after the consideration of the risk management status in the departments, etc. that are subject to audit? Also, does the management team take appropriate measures, such as formulating and implementing improvement measures, with regard to the results of internal audits, and follow up on the improvement status of the audit findings?

(x) Is the management team fully aware that banning and eliminating relations with anti-social forces in a resolute manner is essential for maintaining public trust in Crypto-Asset Exchange Service Providers as well as for the appropriateness of Crypto-Asset Exchange Service Providers' businesses? And has the management team decided a basic policy in light of the details of "Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces" (Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures, issued on June 19, 2007; hereinafter referred to as the "Government Guidelines" in II -1 -2) and declared it both internally and externally?

Moreover, does the management team clearly define the prevention of damage from anti-social forces as one of the issues in the firm's compliance and risk management? For example, are frameworks to realize the basic policy based on the Government Guidelines developed? And is the effectiveness of those systems verified on a regular basis?

(xi) Is the independence of company auditors and the Board of Company Auditors ensured in accordance with the purport of the relevant system? In addition, do company auditors and the Board of Company Auditors properly exercise their extensive authority granted under the law? And do they conduct adequate accounting audits and operational audits? Even when a Board of Company Auditors is organized, does each company auditor stay conscious of their status as a single-person organ and actively perform audit activities under their own responsibility? Moreover, do company auditors and the Board of Company Auditors make efforts to ensure the effectiveness of their own audits by, for example, receiving reports on results of external audits, depending on their details?

(xii) Does the Internal Control Department conduct appropriate monitoring and verification to ensure appropriate business practices for overall business operations in accordance with laws and regulations, as well as internal rules, etc.? In addition, if any serious problem is identified, is it reported to the management team appropriately?

(xiii) Does the Internal Audit Department have any frameworks in place to conduct effective

internal audits independent from the departments that are subject to audit so that sufficient checks can be exercised against the audited departments? In addition, does the Internal Audit Department effectively coordinate with external auditing functions as well as company auditors and the Board of Company Auditors?

(xiv) Does the Internal Audit Department figure out realities of risk management at audited divisions and departments and make efficient and effective internal audit plans? Are those plans designed to fit with the types and severity of risks at appropriate frequencies and depth? Are those plans reviewed and adjusted flexibly according to circumstances? Then, are internal audits conducted efficiently and effectively in accordance with the plans?

(xv) Does the Internal Audit Department report important audit findings to the management team without delay? Does the Internal Audit Department keep track of the improvement status of the audit findings?

II-2 Appropriateness of Business Operations, etc.

II-2-1 Compliance with Laws and Regulations, etc.

II-2-1-1 Legal Compliance Framework, etc.

II-2-1-1-1 Purpose and Significance

It is important for Crypto-Asset Exchange Service Providers to strictly comply with laws, regulations and internal rules, etc. and to endeavor to conduct business operations properly and reliably from the perspective of improving users' trust in the Crypto-Asset Exchange Services and, in turn, improving users' convenience through further distribution and development of Crypto-Assets.

In addition, from the perspective of ensuring appropriate and reliable business operations, Crypto-Asset Exchange Service Providers are required to establish internal rules, etc. for their businesses in accordance with their scale and characteristics; review them constantly; and conduct internal education for officers as well as employees engaged in the Crypto-Asset Exchange Services business and other employees (hereinafter referred to as "officers and employees"). They are also required to verify the status of compliance therewith.

In this regard, even if a Crypto-Asset Exchange Service Provider fails to respond literally as described in each of the supervisory viewpoints in these Guidelines, it is not inappropriate if it is deemed that there are no particular problems from the viewpoint of protecting the interests of users in light of the scale and characteristics of such Crypto-Asset Exchange Service Provider.

When supervising Crypto-Asset Exchange Service Providers, the following points, for example, shall be taken into consideration.

II-2-1-1-2 Major Supervisory Viewpoints

(i) Has the Crypto-Asset Exchange Service Provider regarded compliance as one of the most important management issues and formulated a basic policy to put the recognition into practice, along with a more specific implementation plan (Compliance Program) and a code of conduct (Ethics Code and Compliance Manual), etc.? Also, are these policies, etc. thoroughly known and understood by officers and employees, and are they put into practice in daily business operations?

(ii) When developing a business operation system that is necessary for complying with laws and regulations, etc. based on Article 63-9-3 of the Act and Article 20 (xiii) of the Cabinet Office Order, does the business operation system reflect details of the Association's self-regulatory rules in light of the fact that it is prohibited for Crypto-Asset Exchange Service Providers and their officers and employees to engage in acts that not only violate the Association's self-

regulatory rules, etc., but also lack user protection or may hinder the proper and secure conduct of the Crypto-Asset Exchange Services? For example, referring to the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Services of Employees, etc. Pertaining to the Crypto-Asset Exchange Services," has the Crypto-Asset Exchange Service Provider formulated any service rules based on the details and type of its business, and other rules such as those on prohibited acts of officers and employees?

(iii) Does the Crypto-Asset Exchange Service Provider evaluate and follow up the implementation plan and the code of conduct on a regular basis or as needed? Also, does the Provider review their contents?

(iv) Has the Crypto-Asset Exchange Service Provider established and enhanced a system for training and education on compliance? Does it strive to foster and improve compliance awareness among its officers and employees? In addition, does the Funds Transfer Service Provider make efforts to ensure the effectiveness of the training by, for example, evaluating and following up the training in a timely manner and reviewing the details?

II-2-1-2 Advertising Regulations

II-2-1-2-1 Purpose and Significance

Since the display or representation of advertisements by Crypto-Asset Exchange Service Providers corresponds to the introduction part of the transaction solicitation to users, it is important to provide information through an appropriate display/representation from the viewpoints of preventing users from misidentifying risks as well as discouraging the promotion of speculative transactions. Therefore, when a Crypto-Asset Exchange Service Provider advertises its Crypto-Asset Exchange Services, the Provider is required to clearly and accurately represent the matters specified in Article 63-9-2 of the Act and Article 18 of the Cabinet Office Order, pursuant to Article 17 of the Cabinet Office Order, and is prohibited from making any improper representation pursuant to Article 63-9-3(ii) and (iii) of the Act and Article 20(i) of the Cabinet Office Order.

When supervising Crypto-Asset Exchange Service Providers, in order to confirm whether the appropriateness of the contents and representation of advertisements are ensured, the supervisors shall pay attention to the following points, for example, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Solicitation and Advertisement, etc. Pertaining to the Crypto-Asset Exchange Services."

II-2-1-2-2 Major Supervisory Viewpoints

(1) Scope of advertising

Advertising means informing the general public of a particular matter at any time or on an ongoing basis in order to promote it widely, although it is necessary to make a substantive judgment based on the actual situation for each individual case. For example, it refers to the following.

(A) Television commercials
(B) Radio commercials
(C) Advertising in newspapers, magazines, and other publications
(D) Representation on signboards, standing signboards, placards, bills, etc.
(E) Advertisement towers, billboards, displays on buildings and other workpieces , etc.
(F) Distribution of leaflets, catalogs, pamphlets, leaflets, etc.
(G) Representation on the Internet

Note: An act such as sending an e-mail or direct mail that invites a specific person to perform a specific act constitutes solicitation, even if the act does not fall under the

category of "advertising." Therefore, when soliciting for the conclusion of a Crypto-Asset exchange contract (which refers to the conclusion of a Crypto-Asset exchange contract as stipulated in Article 63-9-3(i) of the Act; the same shall apply hereinafter), it is necessary to pay attention not to violate laws and regulations in light of II-2-1-3.

(2) Clear and accurate representation

In cases where the matters prescribed in each item of Article 63-9-2 of the Act (in the case of Crypto-Asset Exchange Service Providers exclusively managing Crypto-Assets, however, the matters are limited to those prescribed in items (i) and (ii) of the same Article) are represented in advertising, the supervisors shall pay attention to the following points when judging whether or not the clear and accurate representation prescribed in Article 17 of the Cabinet Office Order is made.

(i) Are the size, shape, and colors of letters pertaining to the matter in advertising unduly less conspicuously indicated, compared with letters pertaining to other matters represented in the same advertisement? In particular, with regard to the matters prescribed in Article 63-9 2(iii) of the Act and each item of Article 18 of the Cabinet Office Order, are they indicated in a size that is not significantly different from the largest letter or number in the advertisement?

(ii) Is the matter represented in such a way as to emphasize only the merits of transactions while making the demerits less conspicuous?

(iii) When the advertisement is displayed on a screen, is the representation time ensured long enough to read all the matters to be represented?

(3) Required systems

(i) Has the Crypto-Asset Exchange Service Provider established internal rules, etc. stipulating provisions concerning the handling of advertisements, such as the prevention of inappropriate advertisements, and disseminated them company-wide through internal training, etc. so that its officers and employees properly handle cases in accordance with such internal rules, etc.?

(ii) From the viewpoint of compliance with laws and regulations, has the Crypto-Asset Exchange Service Provider appointed an advertising screening officer to examine advertisements so that appropriate screening is conducted based on screening standards?

II-2-1-3 Prohibited Acts

II-2-1-3-1 Purpose and Significance

Article 63-9-3 of the Act prohibits a Crypto-Asset Exchange Service Provider or its officers and employees from engaging in improper acts when concluding or soliciting the conclusion of a Crypto-Asset exchange contract or when advertising in relation to the Crypto-Asset Exchange Services, or acts specified in Article 20 of the Cabinet Office Order as likely to impair the protection of users of the Crypto-Asset Exchange Services or likely to hinder the proper and secure conduct of the Crypto-Asset Exchange Services.

When supervising Crypto-Asset Exchange Service Providers, in order to confirm whether or not advertising/solicitation and/or receiving orders for transactions, etc. by a Crypto-Asset Exchange Service Provider or its officers and employees have harmed the interests of users or obstructed the proper and secure conduct of the Crypto-Asset Exchange Services, the supervisors shall pay attention to the following points, for example, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Solicitation and Advertisement, etc. Pertaining to the

Crypto-Asset Exchange Services," and "Rules on Development of Order Receipt Management Framework for the Crypto-Asset Exchange Services," etc.

II-2-1-3-2 Major Supervisory Viewpoints

(1) Principle of suitability

(i) When soliciting transactions, based on Article 20(vi) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider ensure that its officers and employees endeavor to conduct appropriate solicitation in accordance with the attributes of the users, etc., by paying attention to the details of the transactions and/or the terms and conditions of the transactions in accordance with the users' knowledge, experience, status of property, age, transaction purpose, risk management recognitional capacity, etc.?

(ii) Has the Crypto-Asset Exchange Service Provider established a user management framework that enables accurate understanding of the attributes, etc. of users and the actual status of transactions, including the following points?

(A) Does the Crypto-Asset Exchange Service Provider appropriately record and preserve user information after sufficiently confirming the user's attributes, such as the purpose of transactions and trading experience, in order to grasp the user's attributes, etc. in a timely and appropriate manner? In addition, when it is ascertained that user attributes, etc. have changed based on an overture from a user, are the details of the recorded user information updated?

(B) Does the Internal Control Department strive to grasp the status of the identification of user attributes, etc. and the status of the management of user information, and verify whether appropriate solicitation is conducted in light of user attributes, etc. as necessary? In addition, does said department strive to establish an environment to ensure its effectiveness, such as reviewing the management method of user information?

(C) For grasping the actual status of transactions by users, does the Crypto-Asset Exchange Service Provider refer to the status of transactions such as trading losses, valuation losses, the number of transactions, and the status of commissions by each user account?

(2) Prohibition of uninvited solicitation

(i) Applicability of uninvited solicitation

(A) "Act of visiting or making a telephone call to solicit the conclusion of a Crypto-Asset exchange contract" prescribed in Article 20(iii) of the Cabinet Office Order includes inquiring whether or not solicitation may be conducted.

(B) A user cannot be deemed to have made a "request to solicit the conclusion of a Crypto-Asset exchange contract" merely because the user who saw advertising, etc. made an inquiry on general matters or requested materials on the outline of the transaction to a Crypto-Asset Exchange Service Provider by telephone, etc.

(ii) Grasping the request status, etc. from each user

(A) Does the Crypto-Asset Exchange Service Provider endeavor to grasp the status of requests from users and the actual status of past transactions, etc. in a timely manner by recording and preserving the data as user information? In addition, when soliciting, does the Crypto-Asset Exchange Service Provider ensure that its officers and employees endeavor to conduct appropriate solicitation in accordance with the status of requests from the respective users and the actual status of past transactions?

(B) A specific handling method should be established for the management of user information,

including the status of requests from users and the status of past transactions, etc. and such method should be disseminated to all officers and employees. In particular, with regard to user information, has the Crypto-Asset Exchange Service Provider established a handling method after thoroughly examining it from the viewpoint of confidentiality, etc.?

(C) Does the Internal Control Department strive to grasp the status of requests from users and the actual status of past transactions, etc. as well as the status of managing user information, and verify, as necessary, whether appropriate solicitation is conducted? In addition, does said department strive to establish an environment to ensure its effectiveness, such as reviewing the management method of user information?

(3) Sales staff management framework

(i) Does the Crypto-Asset Exchange Service Provider appoint the officers and employees in charge of solicitation (hereinafter referred to as "sales staff"), and then provide necessary business guidance and education to ensure appropriate solicitation by the sales staff?

(ii) Has the Internal Control Department established an environment to ensure appropriate solicitation by the sales staff, such as by grasping and verifying the status of solicitation by the sales staff and reviewing their solicitation methods when necessary?

(4) Points of note regarding prevention of unfair acts by officers and employees

(i) Has the Crypto-Asset Exchange Service Provider established an appropriate internal control environment, such as developing the internal rules pertaining to purchase and sale of Crypto-Assets or exchange with other Crypto-Assets and other transactions by its officers and employees?

(ii) Has the Crypto-Asset Exchange Service Provider made efforts for strengthening the sense of compliance with laws and regulations, such as enhancing professional ethics and ensuring full understanding of relevant laws and regulations and the internal rules, aimed at preventing unfair acts by its officers and employees?

(iii) Has the Crypto-Asset Exchange Service Provider taken appropriate measures, such as grasping the actual situation of purchase and sale of Crypto-Assets or exchange with other Crypto-Assets and other transactions by its officers and employees who are in a position to obtain Crypto-Asset related Information (which refers to Crypto-Asset related Information specified in II-2-2-1-2 (5); the same shall apply hereinafter) and reviewing the methods when necessary?

Note: Unfair acts by officers and employees are mainly assumed to be transactions by the officers and employees who fall under Article 20(xi) of the Cabinet Office Order using Crypto-Asset related Information, or transactions by the officers and employees who violate Article 185-22(1), Article 185-23(1) or Article 185-24(1) or (2) of the Financial Instruments and Exchange Act. However, this is not limited to such transactions, and generally includes acts by officers and employees that are prohibited by laws and regulations.

(5) Details of prohibited acts

(i) As "representation misleading the counterparty with regard to the characteristics, etc. of Crypto-Assets" prescribed in Article 63-9-3, Items (i) and (ii) of the Act, the following for example are conceivable.

• Misleading representation concerning a potential risk of loss due to price fluctuations in

Crypto-Assets

- Misleading representation concerning the fact that transfer of the Crypto-Asset is restricted for a certain period based on its structure
- Representation that may mislead users with respect to the financial status of the issuer of Crypto-Assets or the progress of the business conducted by the issuer

(ii) the following are conceivable examples of "representation facilitating purchase and sale of Crypto-Assets or exchange with other Crypto-Assets not for the purpose of using them as payment instruments but solely for seeking profits" prescribed in Article 63-9-3(iii) of the Act.

- Representation which would expressly or implicitly urge people to make a profit, by notably emphasizing the track record and forecast of the Crypto-Asset's price trends
- Act of recommending a transaction not as a means of payment but by inciting gambling, such as introducing a person who has made a profit through purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset, etc.

(iii) the following are conceivable examples of "acts of representation with regard to the characteristics, etc. of Crypto-Assets without providing reasonable supporting grounds" prescribed in Article 20(i) of the Cabinet Office Order.

- Act of using biased analysis to predict price changes of a Crypto-Asset
- Act of representation stating that the Crypto-Asset is safe and low risk on the grounds that it is a Crypto-Asset handled by the Crypto-Asset Exchange Service Provider
- Act of representation stating the soundness of financial conditions, etc., on the grounds that the Crypto-Asset Exchange Service Provider is registered for the Crypto-Asset Exchange Services

(iv) the following are conceivable examples of "acts that violate the articles of incorporation of the Certified Association for Payment Service Providers and other regulations, and that lack sufficient protection of users or are likely to hinder the proper and secure conduct of the Crypto-Asset Exchange Services" prescribed in Article 20(xiii) of the Cabinet Office Order, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Solicitation and Advertisement, etc. Pertaining to the Crypto-Asset Exchange Services," and "Rules on Development of Order Receipt Management Framework for the Crypto-Asset Exchange Services," etc.

- Act of soliciting unspecified and many users to make simultaneous and excessive recommendations of exchange, etc. of specific and a small number of Crypto-Assets continuously for a certain period, which is likely to impair price formation of the Crypto-Assets
- Act of having a user sell Crypto-Assets or exchange them with other Crypto-Assets in excess of the total amount of the Crypto-Assets currently in possession and the remaining Crypto-Assets for which measures have been taken to ensure the delivery of such Crypto-Assets to the user through cover transactions, conclusion of a borrowing agreement, and so on
- Act of providing or guaranteeing a special benefit to a user, etc.

  Note: Mitigation of commissions, etc., provision of premiums and the like, cash-backs, etc. to users, etc. do not fall under "special benefit" immediately. However, it is necessary to pay attention so as to ensure that such acts stay within the scope that is deemed appropriate in general societal terms, such as that the conditions are set based on certain standards and are not unreasonable, that similar treatment is given to other

users who have similar transaction conditions, and that they are not excessive.

- Act of using fraudulent means or committing assault or intimidation at the solicitation of a transaction or receipt of an order
- Act of advertising by using inappropriate places, etc. and time in light of public order and morals
- Act of carrying out a transaction on a user's account without obtaining the user's prior consent;

II-2-1-4 Measures for Verification at the Time of Transaction, etc.

II-2-1-4-1 Purpose and Significance

The establishment of an internal control environment in relation to verification at the time of transaction, preservation of transaction records, notification of suspicious transactions, etc. (which refer to the measures for verification at the time of transaction, etc. prescribed in Article 11 of the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007; hereinafter referred to as "Anti-Criminal Proceeds Act"); hereinafter referred to as "measures for verification at the time of transaction, etc.") bears significant meaning in preventing the abuse of financial services by organized crime groups and in ensuring confidence in the Japanese financial market as well. When supervising Crypto-Asset Exchange Service Providers, the supervisors shall pay attention to the following points, for example, in addition to "Guidelines on Anti-Money Laundering/Terrorist Financing Measures" including a risk-based approach (hereinafter referred to as "Guidelines on Anti-Money Laundering/Terrorist Financing Measures").

Note 1: Transactions by existing customers who have had business relationships with Crypto-Asset Exchange Service Providers prior to the enforcement of the Act for Partial Revision of the Banking Act, etc. to Respond to Changes in the Environment such as Progress of Information and Communications Technology (Act No. 62 of 2016) may not have been verified at the time of transactions, but from the perspective of appropriate customer management, Crypto-Asset Exchange Service Providers are required to endeavor to implement the procedure for the verification at the time of transaction for anyone whose transaction had not been verified at the time of transaction.

Note 2: With regard to the handling of the verification at the time of transaction, it should be noted that necessary measures may be taken separately based on the Anti-Criminal Proceeds Act.

Note 3: Risk-based approach means that Crypto-Asset Exchange Service Providers are expected to identify and assess money laundering and terrorist financing risks to which they are exposed and take appropriate measures to mitigate the risks effectively.

II-2-1-4-2 Major Supervisory Viewpoints

With regards to operations of a Crypto-Asset Exchange Service Provider, the supervisors must check whether the Crypto-Asset Exchange Service Provider has established the following frameworks in order to prevent its exploitation for organized crimes such as terrorist financing and money laundering, by properly taking measures for verification at the time of transaction, etc. and measures listed in the Guidelines on Anti-Money Laundering/Terrorist Financing Measures.

(1) Has the Crypto-Asset Exchange Service Provider developed a centralized control environment for appropriately implementing the measures for verification at the time of transaction and the measures listed in the Guidelines on Anti-Money Laundering/Terrorist Financing Measures? Is

the environment properly functioning?

In particular, has the Funds Transfer Service Provider implemented the following measures in developing the centralized control environment?

Note: In order to appropriately implement measures for verification at the time of transaction, etc., reference must be made to the "Points to Note Concerning the Act on Prevention of Transfer of Criminal Proceeds" (FSA, October 2012).

(i) Whether the Crypto-Asset Exchange Service Provider has selected and appointed an appropriate person as supervisory manager, as stipulated in Article 11(iii) of the Anti-Criminal Proceeds Act, such as a person at a managerial level who is in charge of compliance on measures for terrorist financing and money laundering.

(ii) Whether the Crypto-Asset Exchange Service Provider has taken the following measures in order to research and analyze risks used for terrorist financing and money laundering, etc. and to take action based on the results.

(A) Considering the details of the risk report related to transfer of criminal proceeds, which is prepared and published by the National Public Safety Commission based on Article 3(3) of the Anti-Criminal Proceeds Act, whether the Crypto-Asset Exchange Service Provider properly researches and analyzes the risks in which its own transactions are used for terrorist financing and money laundering, in terms of transaction/commodity characteristics, forms of transactions, countries/regions associated with transactions, customer attributes, etc.; and prepares and regularly reviews documents, etc. describing the results (hereinafter referred to as "risk assessment by a specified business operator, etc.").

(B) Whether the Crypto-Asset Exchange Service Provider collects and analyzes necessary information while considering the details of the risk assessment report by a specified business operator, etc., and continuously scrutinizes the preserved verification records and transaction records, etc.

(C) In conducting transactions for which strict customer management stipulated in the first sentence of Article 4(2) of the Anti-Criminal Proceeds Act is deemed to be particularly necessary, or transactions to which special attention must be given in performing the customer management stipulated in Article 5 of the Regulation for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (hereinafter referred to as "Anti-Criminal Proceeds Enforcement Regulations"), or other transactions in which the risk level of terrorist financing and money laundering is deemed to be high by giving considerations to the details of the risk report related to transfer of criminal proceeds (hereinafter referred to as "high risk transactions"), whether the supervisory manager approves those transactions, and prepares documents describing the results of collected and analyzed information, and stores them together with verification records, transaction records, etc.

(iii) Whether the Crypto-Asset Exchange Service Provider establishes proper policies for recruitment of employees and acceptance of customers.

(iv) Whether the Crypto-Asset Exchange Service Provider conducts necessary audit.

(v) Whether the Crypto-Asset Exchange Service Provider prepares a manual of the customer management method including measures for verification at the time of transaction, etc., disseminates it to employees, and in addition, conducts proper and continuous training to employees so that they can use the manual properly.

(vi) Whether the Crypto-Asset Exchange Service Provider establishes a proper framework (policy, method, information management system, etc.) of reporting regarding matters related to the

abuses of financial services through organized crimes which an employee has found, for example, during verification at the time of transaction or by detecting suspicious transactions.

(2) Has the Crypto-Asset Exchange Service Provider established a control environment for properly performing verification at the time of transaction, such as confirmation of a substantial controller in a transaction with a corporate customer, confirmation of eligibility of foreign PEPs (Note), and proper treatment of identification documents including treatment of personal identification numbers and basic pension numbers?

Note: Foreign PEPs refer to heads of foreign countries and persons occupying an important position in a foreign government, etc. listed in each item of Article 12(3) of the Order for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds (hereinafter referred to as the "Anti-Criminal Proceeds Act Enforcement Order") and in each item of Article 15 of the Anti-Criminal Proceeds Act Enforcement Regulations.

In particular, when conducting transactions for which there is an especially strong necessity for conducting rigid customer management as mentioned in the below (A) through (D), based on the first sentence of Article 4(2) of the Anti-Criminal Proceeds Act and each paragraph of Article 12 of the Anti-Criminal Proceeds Act Enforcement Order, has the Crypto-Asset Exchange Service Provider established an environment in which (re-)verification at the time of transaction is done in a proper manner, such as that a customer's identification matters are confirmed not only in a normal way but also in a more rigid way in which customer identification documents or supplementary documents are additionally received? In addition, when confirmation of the conditions of assets and revenues is obligated, has the Crypto-Asset Exchange Service Provider established an environment in which such confirmation is done in a proper manner?

(A) A transaction in the case where a counterparty to the transaction is suspected of impersonating a customer, etc., or representative, etc., for whom related verification at the time of the transaction is conducted

(B) A transaction with customer, etc., who is suspected of having falsified matters subject to related verification at the time of transaction when such verification has been conducted

(C) A transaction, etc., with a customer, etc., who resides or is located in a country or region in which the establishment of a system to prevent the transfer of criminal proceeds as specified in Article 12(2) of the Anti-Criminal Proceeds Act Enforcement Order is not considered sufficient

(D) A transaction with a customer, etc. who is deemed a foreign PEP

In addition, does the Crypto-Asset Exchange Service Provider properly perform verification at the time of transaction by regarding as specified transactions those into which one transaction is apparently divided in order to reduce the amount of money per transaction below the threshold (the transactions are limited to those listed in each item of Article 7(3) of the Anti-Criminal Proceeds Act Enforcement Order)?

(3) When reporting suspicious transactions, has the Crypto-Asset Exchange Service Provider established an environment for appropriate examination and judgment based on Article 8(2) of the Anti-Criminal Proceeds Act and Articles 26 and 27 of the Anti-Criminal Proceeds Enforcement Regulations? Such examination and judgment should be made after comprehensively considering the customer attributes, the status at the time of transaction, and other specific information held by the Crypto-Asset Exchange Service Provider and related to the

transaction.

Does the Crypto-Asset Exchange Service Provider pay full attention especially to the following points in establishing the environment?

(i) Whether the Crypto-Asset Exchange Service Provider, according to its operations and business profile, has established an environment for detecting, monitoring, and analyzing suspicious customers and transactions, etc. by using the relevant systems and manuals, etc.

(ii) After considering the details of the risk report related to transfer of criminal proceeds, whether the Crypto-Asset Exchange Service Provider fully considers the following aspects: the customer's nationality (whether the customer's home country falls within the FATF's list of non-cooperative countries and territories), eligibility of foreign PEPs, the customer attributes of the business in which the customer is engaging, transaction patterns such as the value and number of transactions in light of the customer attributes, and others. Whether the Crypto-Asset Exchange Service Provider conducts proper confirmation and judgment based on transaction categories such as continuous transactions with existing customers and high risk transactions.

Note 1: When considering and judging the reporting of suspicious transactions, also refer to "Reference Cases on Suspicious Transactions" (Refer to the FSA website.).

Note 2: When introducing a blockchain analysis tool to establish the environment as mentioned in (i) above, the Crypto-Asset Exchange Service Provider should also consider, in (ii) above, the transaction patterns on the blockchain conducted through the addresses, etc. held by its customers.

(4) In cases where the Crypto-Asset Exchange Service Provider exchanges Crypto-Assets with other Crypto-Asset Exchange Service Providers and an overseas service providers, or in cases where the Crypto-Asset Exchange Service Provider permits other Crypto-Asset Exchange Service Providers and overseas service providers to use its in-house developed system, has the Crypto-Asset Exchange Service Provider put the following frameworks in place in accordance with the Guidelines on Anti-Money Laundering/Terrorist Financing Measures?

(i) Whether the Crypto-Asset Exchange Service Provider collects information on the customer base, business details, and the system development status to prevent terrorist financing and money laundering of the relevant Crypto-Asset Exchange Service Providers and the overseas service providers (hereinafter referred to as "transaction parties"), as well as information on the supervisory system for such business operator by the local supervisory authority in the case of the overseas business operators, and appropriately evaluates the risks of being used for terrorist financing and money laundering, etc. of transaction parties. Moreover, whether the Crypto-Asset Exchange Service Provider reviews the above evaluation periodically. In addition, whether the risk evaluation is reviewed as necessary upon the occurrence of new events that could have a significant impact on countermeasures against terrorist financing and money laundering.

(ii) Whether the Crypto-Asset Exchange Service Provider takes appropriate risk mitigation measures such as appropriately screening and judging the conclusion and continuation of contracts relating to transactions with transaction parties, including approval by the supervisory manager.

(iii) Whether the Crypto-Asset Exchange Service Provider clarifies the allocation of responsibility/roles between the Crypto-Asset Exchange Service Provider and transaction parties in relation to the prevention of terrorist financing/money laundering, by means of

documenting such responsibility/roles or any other means.

(5) Has the Crypto-Asset Exchange Service Provider developed the following frameworks, in accordance with the Guidelines on Anti-Money Laundering/Terrorist Financing Measures, when providing services through a partnership with another company or when outsourcing part of its operations related to the Crypto-Asset Exchange Services? When said business partner and the outsourced contractor (hereinafter referred to as "the business partners, etc.") are specified business operators, refer to the matters listed in (4) above.

(i) Whether the Crypto-Asset Exchange Service Provider collects information on the customer base, business details, the system development status to prevent terrorist financing and money laundering of the business partners, etc., and appropriately evaluates the risks of being used for terrorist financing and money laundering, etc. of the business partners, etc. Moreover, whether the Crypto-Asset Exchange Service Provider reviews the above evaluation periodically. In addition, whether the risk evaluation is reviewed as necessary upon the occurrence of new events that could have a significant impact on countermeasures against terrorist financing and money laundering.

(ii) Whether the Crypto-Asset Exchange Service Provider takes appropriate risk mitigation measures such as appropriately screening and judging the conclusion and continuation of the contract with the business partners, etc.

(iii) Whether the Crypto-Asset Exchange Service Provide clarifies the allocation of responsibilities between it and the business partners, etc. in relation to the prevention of terrorist financing/money laundering, by means of documenting such responsibilities or any other means.

(6) In order to prevent unauthorized use, etc. of transactions pertaining to the Crypto-Asset Exchange Services, does the Crypto-Asset Exchange Service Provider examine how to prevent damage due to unauthorized use of transactions pertaining to the Crypto-Asset Exchange Services and take necessary measures, such as performing verification at the time of transaction as necessary, when concluding a contract that describes the continuous or repeated conducts of cash payments and/or the Exchange of Crypto-Assets, etc. as prescribed in Article 2(7) of the Act or a contract that describes the conduct of acts set forth in items (iii) or (iv) of the same paragraph (hereinafter referred to as "account opening contract, etc." or when making any other specified transactions by the Crypto-Asset Exchange Service Provider?

In particular, based on Article 23(1)(ii) of the Cabinet Office Order, the following frameworks need to be put in place for cases where there is a suspicion that a criminal act has been committed with respect to a transaction pertaining to the Crypto-Asset Exchange Services, in consideration of the information provided by investigative authorities, etc. to the effect that the transaction pertaining to the Crypto-Asset Exchange Services has been used for fraud or any other criminal act as well as in light of other circumstances.

(i) Framework to promptly suspend the relevant transaction pertaining to the Crypto-Asset Exchange Services that is suspected of having been used for a criminal act

(ii) Framework to suspend the withdrawal of funds from a person who has concluded an account opening contract, etc. when the person is suspected of using the contract for a criminal act

Note: In a case where a transaction or disbursement of funds pertaining to the Crypto-Asset Exchange Services has been suspended pursuant to (i) or (ii), and where there are reasonable grounds to find that the transaction pertaining to the Crypto-Asset Exchange

Services has been used for a criminal act, or where there are reasonable grounds to find that a person who has concluded an account opening contract, etc. is using the contract for a criminal act, it is desirable to take measures for recovery of damage, such as refunding or returning to the victim the funds and Crypto-Assets related to said transaction pertaining to the Crypto-Asset Exchange Services that is under the management of the Crypto-Asset Exchange Service Provider as well as the funds related to the disbursement of funds.

(7) With regard to the commission of examination issued by a court of unauthorized use of transactions pertaining to the Crypto-Asset Exchange Services and inquiries based on the Attorney Act, etc., has the Crypto-Asset Exchange Service Provider established a framework for making proper judgment of each individual specific case, in line with the purpose of these systems, while considering the confidentiality obligation imposed on the Crypto-Asset Exchange Service Provider?

(8) Has the Crypto-Asset Exchange Service Provider established a framework for appropriately implementing countermeasures against terrorist financing and money laundering at its overseas business locations (branches, overseas subsidiaries, etc.)?

(i) Even at its overseas business locations, does the Crypto-Asset Exchange Service Provider take countermeasures against terrorist financing and money laundering at the same level as in Japan to the extent permitted by local applicable laws and regulation?

Note: In particular, it should be noted that, even at an overseas business location in a country or region to which the FATF Recommendation is not applied or is insufficiently applied, control environments of a similar level as in Japan are required.

(ii) In the case where the country where the overseas business location is situated applies stricter criteria for the countermeasures against money laundering and terrorist financing than in Japan, does it take measures corresponding to such stricter local criteria?

(iii) In the case where the overseas business location is not able to take the countermeasures against money laundering and terrorist financing properly at the same level as in Japan because doing so is prohibited by local laws and regulations, does it promptly provide the following information to the FSA or the Local Finance Office that has jurisdiction over the region where the Crypto-Asset Exchange Service Provider's headquarters is located?

- Name of the country or region
- Specific reasons why it cannot take the countermeasures against terrorist financing and money laundering
- If it takes alternative measures for the countermeasures against terrorist financing and money laundering, the content of such alternative measures.

(9) Does the Crypto-Asset Exchange Service Provider properly implement measures for verification at the time of transaction, etc. by converting the Crypto-Asset pertaining to the transaction into Japanese yen based on the conversion standards that are found to be reasonable, when conducting any of the transactions listed in Article 7(1)(i)(p) and (q) of the Anti-Criminal Proceeds Act Enforcement Order?

The conversion may be carried out, for example, by the following methods, subject to the continued application.

(i) The exchange of a Crypto-Asset with another Crypto-Asset, and the intermediation,

brokerage, or agency thereof.
Conversion method to use the quoting prices of the respective Crypto-Assets subject to said exchange (or the quotation of another Crypto-Assets that can be exchanged with the Crypto-Asset and that can be exchanged with the Japanese currency or a foreign currency in the case of an exchange between the Crypto-Assets with no quotation)

(ii) Transfer of a Crypto-Asset
Conversion method to use the quoting price of the Crypto-Asset subject to said transfer (In the case of transaction of a Crypto-Asset with no quotation, the quotation of another Crypto-Asset that can be exchanged with the Crypto-Asset and that can be exchanged with the Japanese currency or a foreign currency)

With respect to the quotations for Crypto-Assets set forth in (i) and (ii) above, in addition to the prevailing quotations at the time of transaction, the following quotations for example are conceivable.

- Quotations as of the last day of either the month or the week preceding the month or the week in which the transaction date falls, or otherwise as of the first day of either the current month or the current week
- Quotations for a fixed period within one month, such as the average quotation for the month preceding the month in which the transaction date falls or for the preceding week

II-2-1-5 Prevention of Damage that May be Inflicted by Anti-Social Forces

II-2-1-5-1 Purpose and Significance

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important for corporations to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling their social responsibility. It is required for Crypto-Asset Exchange Service Providers as well to exclude anti-social forces from financial transactions in order to prevent not only Crypto-Asset Exchange Service Providers themselves and their officers and employees, but also their users and other stakeholders from suffering damage inflicted by anti-social forces. Needless to say, if Crypto-Asset Exchange Service Providers are to maintain the soundness and appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, Crypto-Asset Exchange Service Providers must strive, on a daily basis, to develop a control system for banning any relations with anti-social forces in accordance with the purpose of the “Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces” (Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures, issued on June 19, 2007).

In particular, anti-social forces in recent times have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly, the management team of Issuers of Prepaid Payment Instruments need to take a resolute stance and implement specific countermeasures.

It should be noted that if a Crypto-Asset Exchange Service Provider delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as threats to the safety of its officers and employees, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the Crypto-Asset Exchange Service Provider and its officers and employees, etc.

(Reference) “Guidelines for Enterprises to Prevent Damage Caused by Anti-Social Forces”

(Agreement at a Meeting of Cabinet Ministers Responsible for Anti-Crime Measures, issued on June 19, 2007)

(i) Basic principles on prevention of damage that may be inflicted by anti-social forces

○ Firm-wide response
○ Cooperation with external expert organizations
○ Ban on any relations, including transactions, with anti-social forces
○ Legal responses, both civil and criminal, in the event of an emergency
○ Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

(ii) Identification of anti-social forces

In judging whether specific groups or individuals constitute "anti-social forces," which are defined as groups or individuals that pursue economic profits through the use of violence, threats, and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to "Boryokudan" crime syndicates, "Boryokudan" affiliated companies, "Sokaiya" racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities, and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms of the nature of their conduct, such as whether they are committing violent acts of demand, or making unreasonable demands that go beyond the limits of legal liability (refer to the "Key Points of Measures against Organized Crime," a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011.)

II-2-1-5-2 Major Supervisory Viewpoints

When examining the control environment of a Crypto-Asset Exchange Service Provider for banning any relationship with anti-social forces and for dissolving any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force in cases where it has established a relationship with an anti-social force unwittingly, as well as the control environment for dealing with unreasonable demands by anti-social forces appropriately, the supervisory authorities, while also giving consideration to the characteristics of specific transactions, shall pay attention to the following points.

(1) Firm-wide response

In light of the need and importance of an action to ban any relationship with anti-social forces organically, does the Crypto-Asset Exchange Service Provider including directors respond to the matter as an organization through appropriate engagement of the management team rather than leaving it solely to the person or department in charge? Does the Crypto-Asset Exchange Service Provider make efforts as a group to eliminate anti-social forces in order to ban the relationship with anti-social forces not only in the Crypto-Asset Exchange Service Provider itself but also in the Crypto-Asset Exchange Services? In addition, does the Crypto-Asset Exchange Service Provider make efforts to eliminate anti-social forces even when providing transactions related to the Crypto-Asset Exchange Services by outsourcing business operations to any other company outside the group or even when providing services through a partnership with any other company outside the group?

(2) Development of a centralized control environment through Anti-Social Forces Response Division

Has the Crypto-Asset Exchange Service Provider established a division in charge of supervising responses to ban any relationship with anti-social forces (hereinafter referred to as "Anti-Social Forces Response Division") so as to develop a centralized control environment for preventing infliction of damage by anti-social forces? Is this division properly functioning?

In particular, does the Funds Transfer Service Provider pay sufficient attention to the following points in developing the centralized control environment?

(i) Does the Anti-Social Forces Response Division actively collect and analyze information on anti-social forces? Has it developed a database to manage such information in a centralized manner? And does it have a system to appropriately update it (such as addition, deletion, or change of information in the database)? Further, is the Anti-Social Forces Response Division making efforts to share information within the group in the process of collecting and analyzing such information, while making active use of information provided by external expert organizations such as the police, the Center for Removal of Criminal Organizations, and lawyers (hereinafter referred to as "external expert organizations")? In addition, does the Anti-Social Forces Response Division have a system to take advantage of information on anti-social forces for screening counterparties of transactions and evaluating the attributes of shareholders of the Crypto-Asset Exchange Service Provider?

(ii) Does the Crypto-Asset Exchange Service Provider make sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the Anti-Social Forces Response Division develop a manual for dealing with anti-social forces, provide on-going training, and foster cooperative relationships with external expert organizations on an ongoing basis? In particular, is the Crypto-Asset Exchange Service Provider prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem?

(iii) Does the Crypto-Asset Exchange Service Provider have a structure in which relevant information is swiftly and appropriately conveyed to the Anti-Social Forces Response Division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands? Further, does the Anti-Social Forces Response Division have a structure to swiftly and appropriately report relevant information to the management team? In addition, does the Anti-Social Forces Response Division have a structure to ensure the safety of individuals encountering anti-social forces in person and to support divisions involved in dealing with them?

(3) Implementation of appropriate prior screening

Does the Crypto-Asset Exchange Service Provider take measures to ban allowing anti-social forces to become a counterparty to a transaction, by conducting appropriate advance screening using information, etc. on anti-social forces to prevent transactions with anti-social forces, and making sure to insert provisions regarding the exclusion of organized crime group in all contracts and terms of transactions?

(4) Implementation of appropriate follow-up review

Has the Crypto-Asset Exchange Service Provider established a framework for conducting an appropriate follow-up review on existing contracts for the purpose of making sure that any

relationships with anti-social forces are eliminated?

(5) Efforts to terminate transactions with anti-social forces

(i) Does the Crypto-Asset Exchange Service Provider have a system under which the information confirming the existence of a transaction with anti-social forces is swiftly and appropriately reported to the management team, including directors, etc., via the Anti-Social Forces Response Division, and response to the situation is made under appropriate directions and involvement by the management team?

(ii) Does the Crypto-Asset Exchange Service Provider encourage termination of transactions with anti-social forces in close cooperation with external expert organizations on an ongoing basis?

(iii) Does the Crypto-Asset Exchange Service Provider take care to prevent the provision of benefits to anti-social forces, such as severing the relationship as soon as possible if the counterparty has been found to be anti-social forces after initiation of a transaction through a follow-up review, etc.?

(iv) Does the Crypto-Asset Exchange Service Provider have a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force?

(6) Dealing with unreasonable demands by anti-social forces

(i) Does the Crypto-Asset Exchange Service Provider have a system under which the information that anti-social forces have made unreasonable demands is swiftly and appropriately reported to the management team, including directors, etc., via the Anti-Social Forces Response Division, and response to the situation is made under appropriate directions and involvement by the management team?

(ii) Does the Crypto-Asset Exchange Service Provider actively consult external expert organizations when anti-social forces make unreasonable demands, and respond to such unreasonable demands based on guidelines set by the Center for Removal of Criminal Organizations and other organizations? In particular, does the Crypto-Asset Exchange Service Provider have a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed?

(iii) Does the Crypto-Asset Exchange Service Provider have a policy to take every possible civil legal action against unreasonable demands by anti-social forces and to avoid hesitating to seek the initiation of a criminal legal action, by proactively reporting damage to the relevant authorities?

(iv) Does the Crypto-Asset Exchange Service Provider ensure that the division in charge of handling problematic conduct promptly conducts a fact-finding investigation upon request from the Anti-Social Forces Response Division, in cases where unreasonable demands from anti-social forces are based on problematic conduct related to business activity or involving any of its officers or employees?

(7) Management of shareholder information

Does the Crypto-Asset Exchange Service Provider manage shareholder information properly, through means such as regularly checking the transaction status of its own shares and examining information regarding the attributes of its shareholders?

II-2-1-6 Supervisory Actions to Misconduct

II-2-1-6-1 Purpose and Significance

In case of occurrence of "an act in violation of laws and regulations with regard to the Crypto-Asset Exchange Services by a director, etc. or an employee, or an act that hinders the sound and appropriate operation of the Crypto-Asset Exchange Services by a director, etc. or an employee" as set forth in Article 41 of the Cabinet Office Order (hereinafter referred to as "misconduct"), the FSA shall take supervisory actions as follows.

Misconduct shall mean and include the following acts in addition to acts in violation of laws and regulations in relation to the business of the Crypto-Asset Exchange Services.

- Fraud, embezzlement, breach of trust, etc. in relation to the business of the Crypto-Asset Exchange Services; which is likely to harm the interests of users thereof
- An act of being subject to a complaint or accusation by a user, or arrest with regard to the business of the Crypto-Asset Exchange Services ; and
- An act equivalent to those listed above that hinders or is likely to hinder the sound and appropriate operation of the business of the Crypto-Asset Exchange Services
- External leakage of one or some of its own Crypto Assets or one or some of user's Crypto Assets that the Crypto-Asset Exchange Service Provider manages based on the business of the Crypto-Asset Exchange Services

II-2-1-6-2 Major Supervisory Viewpoints

(i) When receiving an initial notification of misconduct from a Crypto-Asset Exchange Service Provider, the supervisors shall hold an in-depth interview regarding the facts (the business office where the misconduct occurred, the name, title, and job history of the person who committed such misconduct, a summary of the misconduct, the date when the misconduct was detected, the period of the misconduct, why the misconduct was detected), analysis of the cause of the misconduct, and improvement and response measures against the misconduct, and shall ascertain the following points. The same shall apply to the case where no initial report has been made by a Crypto-Asset Exchange Service Provider but a written notification has been submitted by that Crypto-Asset Exchange Service Provider.

(A) Whether the Issuer of Prepaid Payment Instruments has made a prompt report to the Internal Control Department and a report to the management team in accordance with internal rules, etc.

(B) In cases where the act could constitute a criminal offense, whether the Funds Transfer Service Provider has reported it to the police and other relevant organizations.

(C) Whether the Crypto-Asset Exchange Service Provide has investigated and clarified the misconduct at an independent division (such as the Internal Audit Department).

(ii) The supervisors examines the appropriateness of the business of the Crypto-Asset Exchange Service Provider in relation to the misconduct based on the following viewpoints.

(A) Whether the Crypto-Asset Exchange Service Provider appropriately acted immediately after the misconduct came to light.

(B) Whether the management team has been involved in the misconduct and whether there has been firm-wide involvement.

(C) What impacts the misconduct is expected to have on users of Crypto-Assets.

(D) Whether the internal check-and-balance function is properly working.

(E) Whether the Crypto-Asset Exchange Service Provider has formulated improvement measures to prevent recurrence and sufficient self-cleaning functions, and whether it has

clearly pursued the responsibilities of the parties concerned.

(F) Whether the Crypto-Asset Exchange Service Provider has made appropriate explanations to users of the Crypto-Asset Exchange Services and responded to inquiries.

II-2-2 Provision of Information and Consultation Function, etc. for Protection of Users

II-2-2-1 User Protection Measures, etc.

II-2-2-1-1 Purpose and Significance

Article 63-10(1) of the Act and Articles 21 to 23 inclusive and Article 25 of the Cabinet Office Order require Crypto-Asset Exchange Service Providers to provide information to users at the time of commencement of transactions or conclusion of contracts relating to the Crypto-Asset Exchange Services, provide information when receiving money or Crypto-Assets, etc., and protect users, as well as to take necessary measures (hereinafter referred to as "User Protection Measures, etc.") to ensure the proper and secure conduct of the Crypto-Asset Exchange Services.

When supervising Crypto-Asset Exchange Service Providers, in order to confirm the appropriateness of the development of a framework for implementing User Protection Measures, etc., the supervisors shall grasp details of transactions pertaining to the Crypto-Asset Exchange Services through daily supervisory administration such as interviews, and shall also pay attention to the following points among others.

II-2-2-1-2 Major Supervisory Viewpoints

(1) General viewpoints

(i) In providing explanations and information to users, has the Crypto-Asset Exchange Service Provider established a framework to explain the matters prescribed in Article 21(1), each item of Article 21(2), and Article 22 of the Cabinet Office Order, according to details of transactions, and the form of transactions and the Crypto-Assets, etc. handled?

In addition, has the Crypto-Asset Exchange Service Provider established a framework to provide information in an appropriate manner, such as by issuing written documents (including electromagnetic means) as necessary and then providing an explanation, in light of the knowledge and experience of the relevant users?

Note 1: It should be noted that Article 22(2) of the Cabinet Office Order does not apply to Crypto-Asset Exchange Service Providers that do not conduct the Exchange of Crypto-Assets, etc., and Article 22(3) of the Cabinet Office Order does not apply to Crypto-Asset Exchange Service Providers that do not manage Crypto-Assets.

Note 2: As a framework for providing an explanation according to details of transactions, for example, in cases where multiple transactions are provided, such as selling a Crypto-Asset and then managing the Crypto-Asset, the Crypto-Asset Exchange Service Provider is required to provide an explanation according to the details and terms of each transaction, in accordance with the provisions of the Cabinet Office Order.

Note 3: As a framework for providing an explanation according to the form of transactions, for example, in the case of transactions through the Internet, a method in which the user reads the explanatory matters displayed on the screen of the personal computer operated by the user, clicks a button on the screen after understanding the description, is conceivable. Meanwhile, in the case of face-to-face transactions, a method in which the fact is recorded after delivering a written document or giving an oral explanation is conceivable. Regardless of which method is used, attention shall be paid to ensure that the explanation provides information which the user can clearly

and accurately recognize.

(ii) Has the Crypto-Asset Exchange Service Provider established internal rules, etc. regarding User Protection Measures, etc. specified by laws and regulations, such as the obligation to provide information to users? In addition, has the Provider disseminated them through internal training, etc. so that its officers and employees properly handle cases in accordance with the internal rules, etc.?

(iii) Are the internal check-and-balance functions such as internal control and internal audit properly working to ensure the effectiveness of User Protection Measures, etc.?

(iv) Does the Crypto-Asset Exchange Service Provider make sure to review its business framework for the Crypto-Asset Exchange Services, based on the examination of the effectiveness of User Protection Measures, etc.?

(v) In establishing frameworks for dealing with complaints and consultation, has the Crypto-Asset Exchange Service Provider clearly specified procedures for cases where administrative processing errors have occurred? in addition, has the Provider established a system for smooth processing?

(2) Provision of Information to users

(i) Taking into account the users' knowledge and experience, etc., does the Crypto-Asset Exchange Service Provider appropriately explain about the matters prescribed in Article 21(1), each item of Article 21(2), and Article 22 of the Cabinet Office Order, according to details of transactions, the form of transactions, and the Crypto-Assets, etc. handled?

Note 1: In regard to the "outline and characteristics of Crypto-Assets handled" prescribed in Article 21(2)(iv) of the Cabinet Office Order and the "matters deemed to serve as useful references in regard to the nature of Crypto-Assets" prescribed in item 5 of the same paragraph, the following matters, for example, shall be included, and the contents of the brief explanatory booklet on Crypto-Assets published by the Japan Virtual and Crypto assets Exchange Association shall serve as a reference.

- Main uses of Crypto-Assets
- Matters concerning the mechanism of possession or transfer of Crypto-Assets;
- Respective upper limits, in cases where the total issuance volume of certain Crypto-Assets and the issuable number thereof are capped
- Distribution status of Crypto-Assets
- Risks inherent in Crypto-Assets

Note 2: "Details of the transaction" prescribed in Article 22(1)(iii) of the Cabinet Office Order can include not only the form and method of the transaction but also matters pertaining to the order acceptance and the contract execution for the transaction. (In cases where a difference occurs between the price indicated on the user's order or the price designated by the user at the time of placing the order and the contract price (hereinafter referred to as "slippage"), the details can also include such fact and the cause of such occurrence, and if the occurrence of slippage causes any disadvantage to the user, such fact and details of the event.) Even with regard to a contract or terms of use in which the details of the transaction with a user are specified, the Crypto-Asset Exchange Service Provider should pay attention to ensure that the user's rights and obligations are clearly and accurately recognized.

Note 3: Matters to be explained in accordance with Article 22(1)(iv) of the Cabinet Office Order may include the following, for example.

- Risk of loss or depreciation of a Crypto-Asset due to the bankruptcy of the issuer or administrator, etc. of the Crypto-Asset
- Risk of impairment of rights indicated on a Crypto-Asset due to the failure of the obligor involved in the rights
- Risk of inability to receive the return of a deposited Crypto-Asset due to the bankruptcy of the Crypto-Asset Exchange Service Provider

Note 4: Matters to be explained in accordance with Article 22(1)(v) of the Cabinet Office Order may include the following, for example.
- Risk of loss or depreciation of a Crypto-Asset due to a cyberattacks
- Risk due to blockchain branching

(ii) In cases where a user needs to pay commissions, remuneration, or expenses (hereinafter referred to as "commissions, etc.") to a person other than the Crypto-Asset Exchange Service Provider, does the Provider explain the total amount of commissions, etc., or the maximum amount thereof, or the calculation method thereof, including those for the outsourced contractor?

(iii) Even in cases where a Crypto-Asset Exchange Service Provider conducts a Crypto-Asset margin trading prescribed in Article 1(2)(vi) of the Cabinet Office Order with a user, the Crypto-Asset Exchange Service Provider needs to take into account the user's knowledge and experience, etc. and is required to appropriately explain about the matters prescribed in Article 21(1), each item of Article 21(2), and Article 22 of the Cabinet Office Order, according to details of transactions, the form of transactions, and the Crypto-Assets, etc. handled. Therefore, for example, in cases where a user needs to pay commissions, etc. for the Crypto-Asset margin trading, does the Crypto-Asset Exchange Service Provider explain the total amount of commissions, etc., or the maximum amount thereof, or the calculation method thereof, including those for the Crypto-Asset margin trading?

(iv) In the case where only the maximum amount or the calculation method is explained, not the actual amount of commissions, etc., does the Crypto-Asset Exchange Service Provider make sure to additionally explain about the total estimated amount of commissions, etc. for the user to pay or a calculation example thereof?

(v) In light of the purposes of Article 63(10)(i) of the Act and Article 22 of the Cabinet Office Order, as the matters set forth in Article 22(1)(ix) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider explain, when necessary, matters that serve as references when a user decides whether or not to conclude a contract related to a transaction pertaining to the Crypto-Asset Exchange Services?

Note: Matters to be explained in accordance with Article 22(1)(ix) of the Cabinet Office Order may include the following, for example.
- How to deposit the money and Crypto-Asset related to a transaction pertaining to the Crypto-Asset Exchange Services
- How to confirm the status of the money and Crypto-Asset related to the transaction pertaining to the Crypto-Asset Exchange Services after the transaction request

(vi) As the matters set forth in Article22(4)(iv) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider explain, as necessary, matters that serve as references when a user decides whether or not to conclude an account opening contract, etc.?

Note: Matters to be explained in accordance with Article 22(4)(ix) of the Cabinet Office Order may include the following, for example.

- Matters listed in (v) Note above
- Matters related to the setting of a security code and other security matters
- In cases where an account opening contract, etc. caps the amount that the Crypto-Asset Exchange Service Provider can accept from each user, the upper limit amount

(vii) With regard to a Crypto-Asset for which there is an issuer, as the matters set forth in Article21(2)(v), Article 22(1)(v) and (ix), as well as Article 22(4)(iv) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider explain the following, for example?
- Information regarding the issuer
- Whether the rights and obligations indicated on a Crypto-Asset exist or not, and if they exist, the details
- Calculation base for the selling price

(viii) In cases where a Crypto-Asset Exchange Service Provider is entrusted with the purchase and sale, etc. of Crypto-Assets from a user ("entrustment, etc." as defined in Article 1(2)(iv) of the Cabinet Office Order), and where the Crypto-Asset Exchange Service Provider sometimes acts as the counterparty of the purchase and sale, etc. pertaining to the entrustment, etc., does the Crypto-Asset Exchange Service Provider explain the transaction standards and rules in cases where the Crypto-Asset Exchange Service Provider acts as the counterparty of the transaction, based on Article 22(2)(i) of the Cabinet Office Order?

(ix) When managing users' money or Crypto-Assets, does the Crypto-Asset Exchange Service Provider specifically explain to the effect that it has an obligation to separate the money and the Crypto-Assets deposited by users from the property of the Crypto-Asset Exchange Service Provider itself as a system for protecting users, and the trade name of the trust company, etc. in which the money deposited by users is entrusted or the method of separate management of the Crypto-Assets deposited by users and the Performance-Guarantee Crypto-Assets as provided in Article 63-11-2(1) of the Act, and the name of the person in charge of the above-mentioned management?

(x) Has the Crypto-Asset Exchange Service Provider established procedures for informing and alerting users of security measures and implemented them sufficiently?

Note: The contents of dissemination and alerting of security measures include, for example, anti-virus measures at users' terminals and appropriate setting and management of authentication information such as passwords by users.

(xi) Does the Crypto-Asset Exchange Service Provider verify that information was provided to users in a timely and appropriate manner? In order to conduct such verification, are necessary records, etc. archived?

(xii) Are the contents of information to be provided written in a clear and easy-to-understand manner for users?

(xiii) In cases where information is provided by electromagnetic means or other appropriate means in lieu of delivering documents, does the Crypto-Asset Exchange Service Provider take measures such as allowing users to view or save the content of the provided information for a certain period of time?

(3) Measures for non-face-to-face transactions

(i) Are links of the Crypto-Asset Exchange Service Provider's website configured to prevent a user from misrecognizing a counterparty of transaction? In addition, does the Crypto-Asset Exchange Service Provider take proper anti-phishing measures in a manner befitting its business, such as providing for measures to allow users to verify the authenticity of the

website accessed?

(ii) Does the Crypto-Asset Exchange Service Provider take measures to allow a user to easily confirm and correct the details of his/her instruction concerning a transaction pertaining to the Crypto-Asset Exchange Services, such as displaying the details of the instruction and then requesting the user to confirm the details before sending it to the Crypto-Asset Exchange Service Provider?

(4) Measures to prevent Crypto-Asset Exchange Service Providers from handling inappropriate Crypto-Assets

Based on Article 23(1)(v) of the Cabinet Office Order, in order not to handle Crypto-Assets that are likely to hinder the protection of users or the proper and secure conduct of the Crypto-Asset Exchange Services in light of the characteristics of Crypto Assets and its own business structure, does the Crypto-Asset Exchange Service Provider take the following measures, for example, in light of I-1-2-3 and the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on the Handling of Crypto-Assets"?

(i) When starting to handle a new Crypto-Asset, has the Crypto-Asset Exchange Service Provider established frameworks to identify and evaluate risks that may arise from the handling of the Crypto-Asset (hereinafter referred to as "handling risks") and appropriately examined whether or not the Crypto-Asset should be handled, from the viewpoint of user protection and ensuring the proper and secure conduct of business?

(ii) Does the Crypto-Asset Exchange Service Provider periodically review the details of handling risks concerning Crypto-Assets that it has already handled and then, if necessary, reexamine whether or not the Crypto-Assets should be handled?

(iii) In cases where a Crypto-Asset is to be newly handled or discontinued, does the Crypto-Asset Exchange Service Provider make an organizational decision, such as obtaining the approval of the Board of Directors, based on the results of the examination concerning the handling of the Crypto-Asset?

(iv) Does the department that examines the appropriateness of the handling of Crypto-Assets have a structure in place that enables the appropriate verification of handling risks, such as by making the department independent from the sales department and then assigning personnel with expertise?

(5) Appropriate management of Crypto-Asset related information

Pursuant to Article 23(1)(vi) of the Cabinet Office Order, in order to appropriately manage important information, either concerning Crypto-Assets handled or to be newly handled by a Crypto-Asset Exchange Service Provider or concerning the Crypto-Asset Exchange Service Provider, that is found to have an impact on a user's decisions on the sale and purchase of a Crypto-Asset or the exchange with another Crypto-Asset (excluding cases where such information is readily available to all users of the Crypto-Asset Exchange Services conducted by the Crypto-Asset Exchange Service Provider; hereinafter referred to as "Crypto-Asset related information,") does the Crypto-Asset Exchange Service Provider take the following measures, for example, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on the Establishment of a Management Structure for Crypto-Asset related Information Pertaining to the Crypto-Asset Exchange Services"?

(i) Does the Crypto-Asset Exchange Service Provider have internal rules, etc. that specify the category and scope of information that may fall under Crypto-Asset related information?

Note: The following information may be considered as Crypto-Asset related information.

- Changes in the technical specifications used for the Crypto-Asset such as branching of a blockchain used for the Crypto-Asset, or any other material changes related to the function, utility, or plan of the Crypto-Asset
- Commencement of bankruptcy proceedings, special liquidation proceedings, civil rehabilitation proceedings, corporate reorganization proceedings or other similar insolvency proceedings against the issuer, etc. of the Crypto-Asset, or any other material changes in the business operation or property status of a person or entity that is able to determine the specifications, etc. of the Crypto-Asset
- Decision by Crypto-Asset Exchange Service Providers (including the Crypto-Asset Exchange Service Provider itself) or an overseas business operator, etc. to commence or discontinue the handling of the Crypto-Asset, the occurrence of an event of receiving an order for a large-scale transaction that would have a material impact on the price of the Crypto-Asset, or any other determination or occurrence of an event that would have a material impact on the price or liquidity of the Crypto-Asset
- Occurrence of a security incident that seriously hinders its own conduct of the Crypto-Asset Exchange Services, the commencement of bankruptcy proceedings, or any other decision on or occurrence of a matter that seriously affects its own business operation or status of property pertaining to the Crypto-Asset Exchange Services

(ii) Has the Crypto-Asset Exchange Service Provider established a highly independent department that manages Crypto-Asset related information? In addition, does it have a structure for the department to properly manage Crypto-Asset related information?

(iii) Does the Crypto-Asset Exchange Service Provider have a structure to prevent officers and employees from using Crypto-Asset related information beyond the scope necessary for business purposes or from transmitting such Crypto-Asset related information to a third party when they acquire the information?

(6) Measures in the case of borrowing Crypto-Assets

(i) In indicating the matter prescribed in Article 23(1)(viii) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider make sure to explain the details of the indication in an easy-to-understand manner on the transaction pages, etc. where a user makes a deal to borrow the Crypto-Asset so that the user can clearly and accurately recognize the details of the indication?

(ii) Does the Crypto-Asset Exchange Service Provider properly manage the outstanding balance of debts owed through the borrowing of Crypto-Assets as part of its financial risk management, in light of II-1-2(iv), in order to ensure that such debts do not become excessive in relation to its own repayment capacity or not hinder the repayment of such debts?

(7) Price indication

(i) In indicating the matter prescribed in Article 23(2)(i) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider make sure to explain the details of the indication in an easy-to-understand manner on the transaction pages, etc. where a user makes a deal for purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset so that the user can clearly and accurately recognize the details of the indication?

Note: It should be noted that Article 23(2) of the Cabinet Office Order does not apply to Crypto-Assets Exchange Service Providers that are not engaged in Exchange of

Crypto-Assets, etc.

(ii) Notwithstanding (i) above, when the latest reference price as prescribed in Article 23(2)(i)(a)(2) of the Cabinet Office Order and the price pertaining to the Crypto-Asset handled by the Crypto-Asset Exchange Service Provider at the base time when the latest reference price is calculated as set forth in (i)(a)(1) or (b)(1), (2), and (3) of the same paragraph are compared on the website, etc. of the Association, the latest reference price may be indicated by indicating a link to the website, etc. of the Association on the transaction page where the user makes a deal for purchase and sale of the Crypto-Asset or exchange with another Crypto-Asset. When indicating such a link to the website, etc. of the Association, does the Crypto-Asset Exchange Service Provider make sure to indicate the link information in an easy-to-understand manner on its own transaction page so that the user can clearly and accurately recognize the information?

(8) Measures in the case of providing multiple transaction methods

In cases where multiple transaction methods for Exchange of Crypto-Assets, etc. are provided to a user, does the Crypto-Asset Exchange Service Provider specify, for each type of Crypto-Assets handled, the method to make a transaction under the best condition and the reason for selecting the method, as "the policy and method to execute each user's order for Exchange of Crypto-Assets, etc. under the best terms and conditions for each type of Crypto-Assets" prescribed in Article 23(2)(ii)(a) of the Cabinet Office Order?

Note: The term "cases where multiple transaction methods for Exchange of Crypto-Assets, etc. are provided to a user" refers to cases in which there are multiple methods that the user or the Crypto-Asset Exchange Service Provider can select when executing a transaction. The following situations for example are conceivable.

- Case where the Crypto-Asset Exchange Service Provider conducts a transactions for purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset as the counterparty thereof, while also providing a transaction under entrustment from the user as the intermediary for purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset (hereinafter referred to as a "matching transaction").
- Case where the Crypto-Asset Exchange Service Provider provides a transaction based on entrustment from the user pertaining to the agency service for purchase and sale of a Crypto-Asset or exchange with another Crypto-Asset, and there are two or more candidates for the counterparty
- Case where the Crypto-Asset Exchange Service Provider provides multiple opportunities for matching transactions
- Case where the Crypto-Asset Exchange Service Provider provides multiple transactions with different processing speeds, and commissions, etc.

(9) Conflict-of-interest management system

Based on Article 23(2)(iii) of the Cabinet Office Order, does each Crypto-Asset Exchange Service Provider properly manage transactions in which there is a risk of a conflict of interest between the Crypto-Asset Exchange Service Provider or its stakeholders and users, in accordance with the contents, characteristics, and scale of each Crypto-Asset Exchange Service Provider's business, in order to ensure that the interests of users are not unjustly impaired? To this end, the following measures, for example, may be taken.

(i) Establishment of a system to identify transactions that may cause a conflict of interest

(A) Does the Crypto-Asset Exchange Service Provider identify and categorize transactions that may cause conflicts of interest in advance?

(B) Does the Crypto-Asset Exchange Service Provider have a framework to appropriately reflect the contents, characteristics, and scale of its business when identifying transactions that may cause conflicts of interest?

(C) Does the Crypto-Asset Exchange Service Provider have a framework to periodically verify the validity of specified transactions that are likely to have a conflict of interest, for example, in response to the commencement of new business?

(ii) Methods of conflict-of-interest management

(A) Does the Crypto-Asset Exchange Service Provider have a framework that enables it to select or combine appropriate methods for managing conflicts of interest in accordance with the characteristics of transactions that are likely to cause identified conflicts of interest, while paying attention to, for example, the following points?

- In the case of management through separation of departments, does the Crypto-Asset Exchange Service Provider take strict information blocking measures (system access restrictions and physical blocking measures) among the departments concerned?
- In the case of management through changes in the terms or methods of a transaction or by suspending one transaction, does the Crypto-Asset Exchange Service Provider clarify the responsibility as well as the authority related to the judgment?
- In the case of management by disclosing to a customer that there is a risk of a conflict of interest, does the Crypto-Asset Exchange Service Provider provide any explanation to the customer, in accordance with the attributes of the customer, on the details of the potential conflict of interest and the reasons for selecting the method (including a reason for not choosing other methods) by the time of concluding the contract pertaining to the transaction so that the customer can fully understand the details of the potential conflict of interest and the reasons for selecting the method?
- In the case of management by monitoring the persons sharing information, does an independent division or the like appropriately monitor transactions conducted by such persons?

(B) When the Crypto-Asset Exchange Service Provider and its stakeholders such as its group companies conduct a new transaction, does the Crypto-Asset Exchange Service Provider have a framework to make the necessary check on whether or not any transaction exists that will cause conflicts of interest with the transaction?

(C) Does the Crypto-Asset Exchange Service Provider have a framework to periodically examine its conflict-of-interest management method from the viewpoint of ensuring its effectiveness?

(iii) Formulation and public disclosure of a conflict-of-interest management policy

(A) Does the conflict-of-interest management policy (which refers to the policy prescribed in Article 23(2)(iii) of the Cabinet Office Order), in consideration of the contents, characteristics, and scale of the Crypto-Asset Exchange Service Provider's business, specify the categories of transactions that are likely to cause a conflict of interest, major transaction examples, specific processes for such transactions, methods for managing conflicts of interest (in cases where there are differences in the level and depth of conflict-of-interest management, the details and reasons shall be included), systems for managing conflicts of interest (the responsibility and independence of the person who supervises the company-wide management system for the identification of transactions with a risk of

conflict of interest and the conflict-of-interest management, and a verification system for verifying the identification of transactions with a risk of conflict of interest and the conflict-of-interest management methods), and the scope of stakeholders subject to managing conflicts of interest? In this case, are the category of transactions with potential conflicts of interest, transaction examples, and conflict-of-interest management methods described in correspondence?

(B) When disclosing its conflict-of-Interest management policy, has the Crypto-Asset Exchange Service Provider described in an easy-to-understand manner the category of transactions with a risk of conflict of interest, the conflict-of-interest management methods, the conflict-of-interest management systems, and the scope of stakeholders subject to the conflict-of-interest management, in consideration of the content, characteristics, and scale of the Crypto-Asset Exchange Service Provider's business?

(C) Does the Crypto-Asset Exchange Service Provider properly disclose the conflict-of-interest management policy by means of methods such as posting and showing it at its stores as well as posting it on its website?

(iv) Personnel structure and business operation system

(A) Does the management team recognize the importance of conflict-of-interest management and take the initiative in carrying out such management in good faith?

(B) Does the Crypto-Asset Exchange Service Provider have any document or the like that clarifies the procedures for business operations based on the conflict-of-interest management policy? In addition, does the Crypto-Asset Exchange Service Provider ensure that officers and employees are fully informed of the conflict-of-interest management through measures such as providing training on the conflict-of-interest management policy and the procedures?

(C) Has the Crypto-Asset Exchange Service Provider established a system for identifying transactions that may cause conflicts of interest and for managing conflicts of interest in an integrated manner, such as by appointing a conflict-of-interest management supervisor?

(D) Does the conflict-of-Interest management supervisor identify transactions with potential conflicts of interest and properly manage conflicts of interest in accordance with the conflict-of-Interest management policy, and appropriately verify the effectiveness?

(E) Does the conflict-of-Interest management supervisor secure independence from the sales department and adequately check the Sales Department?

(F) Does the conflict-of-interest management supervisor have any frameworks to aggregate the information necessary for the conflict-of-interest management, including information about transactions by the stakeholders, and adequately manage conflicts of interest?

(G) Does the Crypto-Asset Exchange Service Provider have a framework for periodically verifying the personnel structure and business operation system pertaining to the conflict-of-interest management?

(10) Measures to prevent unfair acts

Based on Article 23(2)(iv) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider investigate whether or not a user has violated Article 185-22(1), Article 185-23(1), or Article 185-24(1) or (2) of the Financial Instruments and Exchange Act, in consideration of the trends in or the details of the user's orders related to Exchange of Crypto-Assets, etc. or the status of Exchange of Crypto-Assets, etc., and other circumstances? If such violation is reasonably suspected, does the Crypto-Asset Exchange Service Provider take the following measures, for

example, as measures to suspend the transactions with the user pertaining to the Crypto-Asset Exchange Services as well as necessary measures to prevent other unfair acts related to Exchange of Crypto-Assets, etc. in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Prevention of Unfair Transactions, etc. Pertaining to the Crypto-Asset Exchange Services"?

Note: The term "other unfair acts related to Exchange of Crypto-Assets, etc" includes acts using Crypto-Assets handled or intended to be handled by the Crypto-Asset Exchange Service Provider or using Crypto-Asset related information concerning the Crypto-Asset Exchange Service Provider for the purpose of benefiting oneself or a third party.

(i) Establishment of a transaction screening system

Has the Crypto-Asset Exchange Service Provider established a necessary system to prevent unfair acts by users, such as by stipulating procedures necessary for conducting transaction screening in internal rules, etc., and establishing a department in charge of transaction screening?

(ii) Accurate understanding of user transaction trends and thorough management

(A) Has the Crypto-Asset Exchange Service Provider formulated a specific handling method for grasping transaction trends, such as the types, transaction methods, and forms of Crypto-Assets to be traded? in addition, based on the handling method, does the Provider accurately understand users' transaction motives, etc. through timely measures such as monitoring?

(B) Has the Crypto-Asset Exchange Service Provider established a framework to ensure the effectiveness of the handling method, such as ensuring that officers and employees are fully informed of the handling method and also reviewing it as necessary?

(C) In cases where the Crypto-Asset Exchange Service Provider suspects that a user is likely to be using a pseudonym account, does the Crypto-Asset Exchange Service Provider make efforts to clarify the identity of the actual trader while also monitoring with particular care?

(iii) Establishment and effective use of transaction screening standards

(A) In order to ensure the fairness of user transactions, has the Crypto-Asset Exchange Service Provider formulated specific sampling criteria that take account of the price percentage changes, transaction status, user transaction patterns, etc. for each type of Crypto-Assets? in addition, does the Provider conduct appropriate sampling based on the criteria?

(B) Does the Crypto-Asset Exchange Service Provider manage such sampled transactions appropriately, through measures such as formulating specific screening standards and taking necessary measures (such as inquiries to the relevant users, reminders, and suspension of transactions) to eliminate unfair transactions by manipulation, etc.?

(C) In regard to the sampling criteria, the screening standards, and the status of measures, does the Internal Control Department have a framework to ensure their effectiveness through means such as verifying their consistency with the actual situation in a timely manner and reviewing them as necessary?

(11) Public disclosure, etc. of a policy on performance of obligations

In managing Crypto-Assets, has the Crypto-Asset Exchange Service Provider stipulated the following matters, for example, as its policy on performance of obligations in cases where the Crypto-Asset Exchange Service Provider is unable to perform all of its obligations pertaining to the management of users' Crypto-Assets that are to be managed separately from its own Crypto-Assets pursuant to the provisions of Article 63-11(2) of the Act, due to the leakage, loss, or

damage of a secret key and other information (hereinafter referred to as "secret key and the like") that are necessary to transfer a Crypto-Asset or any other reasons? in addition, has the Provider publicly disclosed the policy?

- How to perform the obligation
- When to perform the obligation
- Base date for the calculation of the payment amount and the method thereof in cases where the method of performance of the obligation is in the form of money

(12) Other User Protection Measures, etc.

Based on Article 23(1)(i) of the Cabinet Office Order, with respect to the Crypto-Asset Exchange Services, each Crypto-Asset Exchange Service Provider needs to establish frameworks necessary for protecting users of the Crypto-Asset Exchange Services and for ensuring the proper and secure conduct of the Crypto-Asset Exchange Services, in accordance with the characteristics of the Crypto-Assets, the details of transactions, and other circumstances. In this context, has each Crypto-Asset Exchange Service Provider taken the following measures, for example, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association?

(i) Has the Crypto-Asset Exchange Service Provider set criteria for starting transactions and transaction limits, etc., based on transaction details, user attributes, and characteristics of Crypto-Assets it handles?

Note: The user attributes should be determined by taking into account the details listed in II-2-1-3-2 (1) (i). For example, they can be determined based on whether a user is a first-time buyer of a Crypto-Asset or a young person, who has little knowledge and experience in Crypto-Asset transactions, as well as in light of the status of assets held by the user.

(ii) Has the Crypto-Asset Exchange Service Provider established a necessary system to manage transaction orders? In confirming the system, the following points, for example, shall be taken into consideration, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on the Establishment of an Order Management System for the Crypto-Asset Exchange Services."

- Has the Crypto-Asset Exchange Service Provider properly established internal rules based on the above-mentioned self-regulatory rules, and does the Provider make efforts to ensure that all officers and employees are fully informed of them?
- Does the Crypto-Asset Exchange Service Provider have a system that fully functions in order to realize appropriate transactions, for example, by incorporating into the system the establishment of an order limit, including the establishment of a ceiling on orders for transactions?
- Does the Crypto-Asset Exchange Service Provider work on enhancing and maintaining its order management system through the appointment of a person in charge of supervising the transaction system and other staffing, training, and regular inspections, etc.?
- Does the Crypto-Asset Exchange Service Provider have a system under which the relevant manager properly and fully gets involved in order limits? In addition, has the system been implemented appropriately?
- In cases where slippage occurs, does the Crypto-Asset Exchange Service Provider avoid treating the slippage disadvantageously to a user? For example, does the Provider avoid processing the contract by using the price at which the slippage occurs when doing so is disadvantageous to the user, while using the price at which the slippage does not occur when

it is advantageous to the user?

(iii) Does the Crypto-Asset Exchange Service Provider store, for a certain period of time, data on the list prices and contract prices by type of Crypto-Assets it handles?

(iv) Does the Crypto-Asset Exchange Service Provider take necessary measures to prevent the transaction price from deviating significantly from the market price of the Crypto-Asset? In addition, does the Provider take any measures to prevent sudden changes in transaction prices?

II-2-2-2 Responses to Margin Trading

II-2-2-2-1 Purpose and Significance

In cases where a Crypto-Asset Exchange Service Provider conducts a Crypto-Asset margin trading prescribed in Article 1(2)(vi) of the Cabinet Office Order with a user, the Crypto-Asset Exchange Service Provider, pursuant to Article 63-10(2) of the Act and Article 25 of the Cabinet Office Order, needs not only to take the User Protection Measures based on Article 63-10(1) of the Act, but also to provide information on the content of a contract pertaining to the Crypto-Asset margin trading; protect the user of the operations pertaining to the Crypto-Asset margin trading; and take measures to ensure the proper and secure conduct of the business.

Note: For conducting Crypto-Asset margin trading, in cases where a Crypto-Asset Exchange Service Provider lends money to users, the Provider needs to register itself as a money lending service provider.

Crypto-Asset margin trading can be considered to have the same economic functions and risks as Crypto-Asset derivatives trading, in that it enables the leveraged trading on the basis of the source fund (security deposit) by receiving credit from the Crypto-Asset Exchange Service Provider with the security deposit (referring to security deposit as stipulated in Article 25(1)(i) of the Cabinet Office Order; the same shall apply hereinafter) as the collateral. As described above, since Crypto-Asset margin trading may invite excessive speculation, the supervisory authorities shall request, when necessary, the Crypto-Asset Exchange Service Provider engaged in such Crypto-Asset margin trading to establish a business operation framework equivalent to that of any Financial Instruments Business Operator or the like engaged in Crypto-Asset derivative trading, based on the details or form of the margin trading provided by the Crypto-Asset Exchange Service Provider, and shall pay attention to the following points, for example.

II-2-2-2-2 Major Supervisory Viewpoints

(1) Provision of information to users

(i) Concerning “the amount of the security deposit for a user of Crypto-Asset margin trading to deposit and the calculation method thereof” as provided for in Article 25(1)(i) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider explain the fact that the amount of the security deposit from the user fluctuates due to fluctuations in market prices, etc., the calculation method thereof, and matters concerning additional security deposit (hereinafter referred to as “additional deposit”) that must be deposited if the amount falls short of the required amount due to fluctuations in the amount of the security deposit?

(ii) Does the Crypto-Asset Exchange Service Provider explain “when there is a risk that the amount of loss concerning Crypto-Asset margin trading might exceed the amount of the security deposit set forth in the preceding item, to that effect and the reason therefor” as prescribed in Article 25(1)(ii) of the Cabinet Office Order? To put it more specifically, does

the Provider explain the following matters?

(A) In cases where there is a risk that a loss exceeding the amount of the security deposit may be incurred due to rapid fluctuations in the market even if a loss-cut transaction (which refers to the loss-cut transaction set forth in Article 25(5)(iii) of the Cabinet Office Order; the same shall apply hereinafter) is conducted, to that effect

(B) In cases where a Crypto-Asset is substituted as the whole or part of a security deposit in accordance with Article 25(6) of the Cabinet Office Order (hereinafter referred to as "substitute Crypto-Asset"), if there is a risk that a loss exceeding the amount of the security deposit will be incurred due to a decrease in the amount of the security deposit in the wake of a decline in the value of the Crypto-Asset, to that effect

(iii) Does the Crypto-Asset Exchange Service Provider also explain the repayment due date of the obligation pertaining to credit granting for Crypto-Asset margin trading in cases where a loss-cut transaction has been arranged, as the "repayment due date" prescribed in Article 25(1)(iii) of the Cabinet Office Order?

(iv) In light of the purposes of Article 63-10(2) of the Act and Article 25 of the Cabinet Office Order, as the matters set forth in Article25(1)(iv) of the Cabinet Office Order, does the Crypto-Asset Exchange Service Provider explain, as necessary, matters that serve as references when a user decides whether or not to conclude a contract related to the Crypto-Asset margin trading?

Note: Matters to be explained in accordance with Article 25(1)(iv) of the Cabinet Office Order may include the following, for example.

(A) The fact that arrangements for the loss-cut transaction have been made, and the details thereof

(B) Counterparty of the cover transaction and the outline thereof

(C) In cases where a Crypto-Asset margin trading is to be compulsorily settled when an additional deposit is not deposited by the prescribed due date, to that effect; and in cases where there is a risk of loss arising from such compulsory settlement, to that effect

(D) In cases where the whole or part of money or Crypto-Assets acquired by a user through Crypto-Asset margin trading serves as the collateral for the obligation pertaining to the credit granting for the Crypto-Asset margin trading, to that effect

(2) Security deposit management

(i) Does the Crypto-Asset Exchange Service Provider include security deposits deposited by users in the scope of separate management based on Article 63-11 of the Act and Article 26 and Article 27 of the Cabinet Office Order, and appropriately handle such deposits under the separate management in accordance with II-2-2-3?

Note: Money or a Crypto-Asset acquired by a user through Crypto-Asset margin trading that has been provided as the collateral for the obligation pertaining to the credit granting for the Crypto-Asset margin trading is not required to be managed by the method specified in Article 63-11(1) and (2) of the Act.

(ii) Based on Article 25(5)(i) and (ii) of the Cabinet Office Order, when conducting Crypto-Asset margin trading, does the Crypto-Asset Exchange Service Provider require the user to deposit a security deposit of not less than the amount corresponding to the following categories in advance?

(A) Crypto-Asset margin trading for individuals

Amount obtained by multiplying the amount of Crypto-Asset margin trading (or the total

amount in cases where the calculation is made for multiple transactions in a lump sum) that the user intends to conduct or will conduct by 50/100

(B) Crypto-Asset margin trading for corporations

Amount obtained by multiplying the amount of Crypto-Asset margin trading (or the total amount in cases where the calculation is made for multiple transactions in a lump sum) that the user intends to execute or will execute by the assumed risk ratio (which refers to of the assumed risk ratio of a Crypto-Asset prescribed in Article 25(5)(ii) of the Cabinet Office Order; the same shall apply hereinafter) of the Crypto-Asset or the combination of Crypto-Assets for the Crypto-Asset margin trading (In cases where a Crypto-Asset Exchange Service Provider does not use any assumed risk ratio of Crypto-Assets, the amount shall be obtained by multiplying the amount of the Crypto-Asset margin trading by 50/100.)

(iii) Does the Crypto-Asset Exchange Service Provider properly calculate the respective amounts of security deposits deposited by individual users on each business day? In addition, when a substitute Crypto-Asset is deposited as the whole or part of a security deposit, does the Crypto-Asset Exchange Service Provider appropriately calculate the substitution price in accordance with the rules of the Association after measuring the Crypto-Asset at market value every business day?

Also, when making a calculation about a security deposit from a user, does the Crypto-Asset Exchange Service Provider add or subtract the respective amounts listed in (A) and (B) below from the money or the substitute Crypto-Asset deposited by the user?

(A) Realized gain or loss

(B) Valuation gain or loss

(iv) In cases where the amount of a security deposit calculated based on (iii) above falls short of the amount corresponding to the following categories, does the Crypto-Asset Exchange Service Provider make sure to have the user promptly deposit an additional amount of the shortfall pursuant to Article 25(5)(i) and (ii) of the Cabinet Office Order?

Note: An additional deposit of the shortfall shall be made within 48 hours from the time of determination of the shortfall, except for unavoidable cases such as the inability to contact the user.

(A) Crypto-Asset margin trading for individuals

Amount obtained by multiplying the amount of Crypto-Asset margin trading (or the total amount in cases where the calculation is made for multiple transactions in a lump sum) that the user executes by 50/100

(B) Crypto-Asset margin trading for corporations

Amount obtained by multiplying the amount of Crypto-Asset margin trading (or the total amount in cases where the calculation is made for multiple transactions in a lump sum) that the user conducts by the assumed risk ratio of the Crypto-Asset or the combination of Crypto-Assets for the Crypto-Asset margin trading (In cases where a Crypto-Asset Exchange Service Provider does not use any assumed risk ratio of Crypto-Assets, the amount shall be obtained by multiplying the amount of the Crypto-Asset margin trading(s) by 50/100)

(3) Points to note regarding Crypto-Asset assumed risk ratio in Crypto-Asset margin trading for corporations

(i) In cases where the Crypto-Asset Exchange Service Provider calculates the Crypto-Asset

assumed risk ratio by itself

(A) Does the Crypto-Asset Exchange Service Provider have established a model (referring to the quantitative calculation model set forth in the "Matters on Establishment of Calculation Methods for Crypto-Asset Assumed Risk Ratio Pertaining to Crypto-Asset Margin Trading"; the same shall apply in (ii) below) that ensures accuracy and rationality and have developed a control environment to calculate the Crypto-Asset assumed risk ratio based on data continuously calculated by a reasonable method?

(B) Does the Crypto-Asset Exchange Service Provider have developed a control environment to verify the Crypto-Asset assumed risk ratio calculated using the model ex post facto as well as every time the ratio is calculated and to review the model as necessary?

(ii) In cases where the Crypto-Asset Exchange Service Provider outsources the calculation of the Crypto-Asset assumed risk ratio

(A) Does the Crypto-Asset Exchange Service Provider monitor whether the outsourced contractor has constructed a model that ensures accuracy and rationality and has a framework to calculate the Crypto-Asset assumed risk ratio based on data continuously calculated by a reasonable method?

(B) Does the Crypto-Asset Exchange Service Provider monitor whether the outsourced contractor has developed a control environment to verify the Crypto-Asset assumed risk ratio calculated using the model ex post facto as well as every time the ratio is calculated and to review the model as necessary?

(C) In cases where an outsourced contractor entrusts the whole or part of outsourced business in (A) and (B) above to its subcontractor(s), does the Crypto-Asset Exchange Service Provider check whether the outsourced contractor is adequately supervising such subcontractor(s)? In addition, does the Crypto-Asset Exchange Service Provider directly monitor the subcontractor(s) as necessary?

(D) In cases where the Association calculates and publicly discloses any Crypto-Asset assumed risk ratio (including cases where the Association entrusts part or all of the calculations and public disclosures of such ratio), and also in cases where a Crypto-Asset Exchange Service Provider uses the ratio, does the Crypto-Asset Exchange Provider have a framework to accurately and continuously use the ratio?

Note: In the above (D), the supervisory authorities shall verify whether the Association conducts proper business operations.

(4) Loss-cut transactions in Crypto-Asset margin trading for individuals

(i) Has the Crypto-Asset Exchange Service Provider established a certain level at which it executes a loss-cut transaction in consideration of price fluctuation risk, and liquidity risk, etc., so that the loss to a user will not exceed the user's security deposit?

(ii) Has the Crypto-Asset Exchange Service Provider formulated internal rules, etc. that clearly stipulate arrangements concerning loss-cut transactions, and reflected them in contracts with users?

(iii) Does the Crypto-Asset Exchange Service Provider appropriately grasp the respective positions of users at each time during trading hours and execute loss-cut transactions without exception in cases where the level described in (i) above is hit?

(iv) Does the Crypto-Asset Exchange Service Provider report the execution status of loss-cut transactions to the Board of Directors, etc. on a regular or as needed basis?

(5) Establishment of a system to ensure the protection of users and the proper and secure conduct of business

Based on Article 25(5)(iv) of the Cabinet Office Order, with respect to the Crypto-Asset margin trading, each Crypto-Asset Exchange Service Provider needs to establish frameworks necessary for protecting users of business pertaining to Crypto-Asset margin trading and for ensuring the proper and secure conduct of the business, in accordance with the details of the Crypto-Asset margin trading and other circumstances. In this context, has each Crypto-Asset Exchange Service Provider taken the following measures, for example?

(i) If requested by the user, does the Crypto-Asset Exchange Service Provider provide in a timely and appropriate manner information that is needed for the user to settle his/her accounts, etc.? For example, does the Crypto-Asset Exchange Service Provider provide or notify market price information on the user's position at a particular time on a periodic or as-needed basis?

(ii) When a user deposits substitute Crypto-Assets as the whole or part of his/her security deposit, does the Crypto-Asset Exchange Service Provider make sure to have the user deposit sufficient quantities of Crypto-Assets exceeding the required amount, taking into account the price fluctuation risk of the substitute Crypto-Assets?

(iii) Based on II-1-2(iv), as part of financial risk management, does the Crypto-Asset Exchange Service Provider appropriately manage the credit risk pertaining to Crypto-Asset margin trading users and the price fluctuation risk of the Provider's positions obtained from its Crypto-Asset margin trading?

(iv) Has the Crypto-Asset Exchange Service Provider taken necessary measures to prevent conflicts of interest, based on the fact that margin trading is likely to be used for excessive speculative trading, and that if the Provider has dual functions as an operator of a trading platform on one hand and as a provider of funds, etc. to its customers on the other hand, it may be difficult to prevent price fluctuations associated with excessive speculation under the former function because of the conflicts of interest between the dual functions?

II-2-2-3 Separate Management of Money, Crypto-Assets, and Performance-Guarantee Crypto-Assets Deposited by Users

II-2-2-3-1 Purpose and Significance

When Crypto-Asset Exchange Service Providers receive deposits of money or Crypto-Assets from users, they are required to secure proper handling of the separate management of such users' money and Crypto-Assets (hereinafter referred to as the "Users' Property") and the Performance-Guarantee Crypto-Assets (referring to the Performance-Guarantee Crypto-Assets prescribed in Article 63-11-2(1) of the Act; the same shall apply hereinafter) pursuant to Article 63-11 and Article 63-11-2 of the Act as well as Articles 26, 27, and 29 of the Cabinet Office Order.

When supervising Crypto-Asset Exchange Service Providers, in order to confirm the appropriateness of their separate management of the Users' Property and Performance-Guarantee Crypto-Assets (hereinafter referred to as "Users' Property, etc."), it is necessary to require them to submit a report on an external audit and internal audit on a regular or as needed basis as well as to pay attention to the following points based on the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Management of Users' Property relating to the Crypto-Asset Exchange Services" and the regulations, etc. designated by the Commissioner of the Financial Services Agency as prescribed in Articles 28 and 30 of the Cabinet Office Order.

II-2-2-3-2 Major Supervisory Viewpoints

(1) Recognition and involvement of the management team

Does the management team of the Crypto-Asset Exchange Provider recognize the importance of the separate management of the User's Property, etc., based on the understanding that separate management of the Users' Property, etc. contributes to user protection? Also, does the management team receive a report on the status of the separate management of the Users' Property, etc. on a regular or as-needed basis and use it in developing a system to properly implement the separate management of the Users' Property, etc. (including the establishment of an internal checking function)?

(2) General viewpoints relating to separate management

(i) Do the internal rules of the Crypto-Asset Exchange Service Provider specifically provide for how to implement the separate management for each type of money and Crypto-Assets? In addition, are they reflected in the contract with each user?

(ii) Does the Crypto-Asset Exchange Service Provider clearly separate money and Crypto-Assets, which is its own property, from the Users' Property, etc. based on the implementation methods set forth in (i) above? And can the balance of money and/or the quantity of Crypto-Assets of individual users be ascertained immediately? Does the Crypto-Asset Exchange Service Provider properly verify its compliance status?

(iii) Are the Crypto-Assets that the Crypto-Asset Exchange Service Provider holds as its own property and the Performance-Guarantee Crypto-Assets clearly separated based on the implementation methods in (i) above? In addition, is it possible to identify immediately which one is the Performance-Guarantee Crypto-Assets? Does the Crypto-Asset Exchange Service Provider properly verify its compliance status?

(iv) Does the Crypto-Asset Exchange Service Provider manage users' money based on the contract pertaining to the Segregated User Management Trusts that satisfy the requirements of each item of Article 26(1) of the Cabinet Office Order? And does the Crypto-Asset Exchange Service Provider calculate the individual amount of segregated user management and the required amount of segregated user management prescribed in item (vi) of the same paragraph every business day pursuant to the provision of paragraph (2) of the same Article?

(v) Has the Crypto-Asset Exchange Service Provider established a department that is responsible for the separate management businesses? And does the Crypto-Asset Exchange Service Provider appoint those responsible for acceptance and payment of the Users' Property, etc. and those responsible for crosschecking the balance of the Users' Property, etc. by each type of money and Crypto-Assets, and then prohibit these persons responsible from engaging in the two functions at the same time? In addition, does the Crypto-Asset Exchange Service Provider take measures to relocate and shift the persons responsible on a regular basis from the perspectives of preventing problematic conducts and wrongful acts?

(3) Supervisory viewpoints regarding separate management of Crypto-Assets deposited by users (hereinafter referred to as the "Entrusted Crypto-Assets") and Performance Guarantee Crypto-Assets

(i) With regard to separate management in the case where Entrusted Crypto-Assets and Performance Guarantee Crypto-Assets (hereinafter referred to as the "Target Crypto-Assets") are managed by the Crypto-Asset Exchange Service Provider itself, does the Provider make sure to manage the Target Crypto-Assets in a different wallet from the wallet in which its own

Crypto-Assets (excluding Performance Guarantee Crypto-Assets; hereinafter the same shall apply in (i)) are managed? Does the Crypto-Asset Exchange Service Provider store the wallet for managing its own Crypto-Assets and the wallet for managing the Target Crypto-Assets in clearly segregated storages, respectively? For example, one conceivable way is to clearly separate devices for storing the wallets.

(ii) With regard to separate management in the case where management of the Target Crypto-Assets is entrusted to a third party, does the Crypto-Asset Exchange Service Provider make sure to have the third party manage the Target Crypto-Assets in a different wallet from the wallet in which Crypto-Assets other than the Target Crypto-Assets are managed? Does Crypto-Asset Exchange Service Provider have the third party store the wallet for managing the Target Crypto-Assets and the wallet for managing Crypto-Assets other than the Target Crypto-Assets in clearly segregated storages, respectively? For example, one conceivable way is to clearly separate devices for storing the wallets.

(iii) With regard to the management of the Target Crypto-Assets, has the Crypto-Asset Exchange Service Provider taken necessary measures to prevent a situation in which the current quantity of the Target Crypto-Assets on networks such as a blockchain falls short of the balance of the Target Crypto-Assets on the books managed by the Crypto-Asset Exchange Service Provider due to circumstances such as a case where transaction details are not reflected in networks such as a blockchain?

Note: In light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Management of Users' Property relating to the Crypto-Asset Exchange Services," conceivable necessary measures, for example, can include a measure by which the Crypto-Asset Exchange Service Provider stipulates in its internal rules the quantity of Crypto-Assets necessary to prevent a situation in which the current quantity of the Target Crypto-Assets on networks such as a blockchain falls short of the balance of the Target Crypto-Assets on the books managed by the Crypto-Asset Exchange Service Provider, while also commingling its own Crypto-Assets of the same type and up to the same quantity as the relevant Crypto-Assets' in the wallet for managing the Target Crypto-Assets. (If the commingling exceeds said quantity, such commingling must be eliminated within five business days from the day following the date of occurrence.)

(iv) With regard to the management of the Target Crypto-Assets, does the Crypto-Asset Exchange Service Provider reconcile the balance of the Target Crypto-Assets on the books managed by the Provider and the current quantity of the Target Crypto-Assets on networks such as a blockchain every business day? In addition, in cases where the reconciliation has revealed the current quantity of the Target Crypto-Assets is less than the balance of the Target Crypto-Assets on the books, despite the measure set forth in (iii) above, does the Crypto-Asset Exchange Service Provider analyze the cause and promptly resolve the shortfall?

Note: Such shortfall shall be resolved within five business days (in the case where the user can pay out the Entrusted Crypto-Assets within a period shorter than five business days based on the contract, such period) from the day immediately following the day of such shortfall.

(v) In cases where the Crypto-Asset Exchange Service Provider manages the Target Crypto-Assets on its own, does the Provider adopt any appropriate management methods to prevent the Target Crypto-Assets from being leaked to the outside, such as by recording and managing the secret keys, etc. necessary for transferring the Target Crypto-Assets on electronic devices

that are always unconnected to the Internet, or by means of other equivalent technical security measures, except for the Entrusted Crypto-Assets that satisfy the requirements specified in Article 63-11(2) of the Act and Article 27(2) of the Cabinet Office Order (hereinafter referred to as the "Target Entrusted Crypto-Assets")? Note that electronic devices, etc. that have been connected to the Internet even once do not fall under "electronic devices, etc. that are always unconnected to the Internet".

Note: Whether an "equivalent technical security measure" has been taken needs to be substantively determined for each individual case in light of the actual situation. However, as an example, the following case is conceivable: While secret keys, etc. necessary to transfer Target Crypto-Assets are recorded and managed in an electronic device, etc. connected to the Internet only at the time of signature, the secret keys, etc. recorded in such electronic device, etc. are in a technical specification that can be signed in such electronic device, etc. without being transferred from such electronic device, etc. to the outside at all, and moreover the authenticity of transaction details is confirmed each time, as they are made by manually signing with such secret keys, etc.

(vi) In cases where a Crypto-Asset Exchange Service Provider entrusts the management of the Target Crypto-Assets to a third party, does the third party manage the Target Crypto-Assets, except for the Target Entrusted Crypto-Assets, in a manner that is reasonably deemed to ensure the same level of the user protection as in the case where the Crypto-Asset Exchange Service Provider manages them on its own, in terms of protection of the Target Crypto-Assets?

Note: Whether the manner corresponds to "a manner that is reasonably deemed to ensure the same level of the user protection as in the case where the Crypto-Asset Exchange Service Provider manages them on its own" needs to be substantively determined for each individual case in light of the actual situation. However, for example, the following cases are conceivable.

- Case where a Crypto-Asset Exchange Service Provider entrusts the management of the Target Crypto-Assets to another Crypto-Asset Exchange Service Provider and where there is an agreement that the Target Crypto-Assets under the management of the other Crypto-Asset Exchange Service Provider will be promptly returned to the entrusting Crypto-Asset Exchange Service Provider in the event of the bankruptcy of the entrusting Crypto-Asset Exchange Service Provider or on the occurrence of other certain causes
- Case where a Crypto-Asset Exchange Service Provider entrusts the Target Crypto-Assets to a trust company or the like and where the respective users of the Crypto-Asset Exchange Service Provider will receive the Target Crypto-Assets in trust as the beneficiaries in the event of the bankruptcy of the Crypto-Asset Exchange Service Provider or on the occurrence of certain other causes

(vii) Upon the occurrence of a situation where the whole or part of the Target Crypto-Assets excluding the Target Entrusted Crypto-Assets are managed by methods other than those described in (v) and (vi) above, does the Crypto-Asset Exchange Service Provider resolve the situation within one business day from the day following the day on which the situation occurred?

(viii) In cases where a Crypto-Asset Exchange Service Provider entrusts management of the Target Crypto-Assets to a third party, does the Crypto-Asset Exchange Service Provider confirm that the entrusted third party complies with the matters listed in (2)(i) through (iii) and (v) above

as well as (3)(ii) through (iv), (vi) and (vii) above, and that necessary responses to leakage risks are taken in accordance with II-2-2-4?

(4) Separate Management Audits

(i) Does the Crypto-Asset Exchange Service Provider have necessary internal frameworks to deal with Separate Management Audits (which collectively refer to the separate management audit prescribed in Article 28(1) of the Cabinet Office Order and the audit of separate management of Performance Guarantee Crypto-Assets prescribed in Article 30 of the Cabinet Office Order; the same shall apply hereinafter)? (Such frameworks include, but are not limited to, the formulation of internal rules and manuals, and the establishment of response divisions.)

(ii) Are important matters identified and pointed out in Separate Management Audits reported without delay to the Board of Directors and company auditors or the Board of Company Auditors?

(iii) Are matters pointed out in Separate Management Audits improved within a certain period of time? In addition, does the Internal Audit Department properly grasp and verify the improvement status of the audit findings?

Note: Audit reports must be submitted to the competent Local Finance Bureau within four months from the base date of Separate Management Audits, in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on the Management of Users' Property Pertaining to the Crypto-Asset Exchange Services."

II-2-2-4 Responses to the Risk of Crypto-Asset Leakage

II-2-2-4-1 Purpose and Significance

When a Crypto-Asset Exchange Service Provider receives a Crypto-Asset as a deposit from a user, there is a risk that the Crypto-Asset Exchange Service Provider may not be able to return the Crypto-Asset to the user due to the leakage of the Crypto-Asset due to unauthorized access, etc., and thus the user may not be protected. Therefore, even in normal times, Crypto-Asset Exchange Service Providers are required to appropriately respond to such leakage risk through the development of internal control environments (including an internal audit environment suited to the nature of business) such as separate management and IT system risk management.

In fact, there have been multiple cases in which large amounts of Crypto-Assets have been leaked due to unauthorized access, etc., and thus the response to the risk of such leakage has become one of the most important issues in the management of Crypto-Asset Exchange Service Providers.

When supervising Crypto-Asset Exchange Service Providers, in order to confirm whether they have been appropriately responding to the risk of the above-mentioned leakage, the supervisors shall pay attention to the following points, for example.

II-2-2-4-2 Major Supervisory Viewpoints

(1) Recognition and involvement of the management team

Does the management team of the Crypto-Asset Exchange Provider recognize the importance of the response to the leakage risk, based on the understanding that the response to the leakage risk contributes to user protection? In addition, does the management team utilize reported information in developing a system to appropriately respond to the leakage risk through measures such as receiving reports on the response status to the leakage risk on a regular or as needed basis?

(2) Identification and evaluation of the leakage risk

(i) Does the Crypto-Asset Exchange Service Provider identify and evaluate the Crypto-Asset leakage risk for each type of Crypto-Assets it handles?

Note: It should be noted that guidelines on security measures by the Association and related organizations with expert knowledge should also be referred to when identifying and evaluating the leakage risk.

(ii) In identifying the leakage risk, does the Crypto-Asset Exchange Service Provider, after taking into consideration circumstances such as the structure of the Crypto-Assets, the technology used for the Crypto-Assets, the internal system and network environment, and the operation leading to the use (signature) of the secret keys, etc. necessary for transferring the Target Crypto-Assets, uncover possible leakage situations (including, but not limited to, leakage, theft, unauthorized use, and loss of the secret key, etc.) and specifically identify the risks causing the leakage (including but not limited to clerical errors, internal fraud, and system malfunctions, in addition to cyberattacks)?

(iii) In evaluating the specified leakage risk, does Crypto-Asset Exchange Service Provider specifically analyze and evaluate the impact on the Target Crypto-Assets and other impacts on users and on its management that may arise from the exposure of the risk? Also, does the Crypto-Asset Exchange Service Provider periodically review its risk evaluation? In addition, does the Provider make sure to review the risk assessment as necessary on the occurrence of a new event that could have a significant impact on the management of the Target Crypto-Assets?

(iv) In cases where the Crypto-Asset Exchange Service Provider starts to handle a new Crypto Asset or to provide a new service, does it analyze the Crypto-Asset or the service, etc. prior to the provision and conduct the validation from the viewpoint of the leakage risk?

(3) Reduction of the leakage risk

(i) In cases where the Crypto-Asset Exchange Service Provider has no choice but to manage the secret key(s), etc. in an environment connected to the Internet for reasons such as user convenience, does the Provider, within the scope of the requirements prescribed in Article 63-11(2) of the Act and Article 27(2) of the Cabinet Office Order, take measures, such as stipulating in the internal rules the upper limit of the Entrusted Crypto-Assets whose secret keys, etc. are managed in said environment, and then managing the secret keys, etc. within said upper limit?

(ii) In addition to (i) above, in order to reduce the leakage risk, Crypto-Asset Exchange Service Providers need to refer to guidelines on security measures by the Association and related organizations with expert knowledge, while also taking into account changes in the leakage patterns and the technological progress, etc. Have they taken effective measures to reduce the leakage risk identified and evaluated in (2) above, including the following points, for example?

(A) In cases where a Crypto-Asset Exchange Service Provider transfers a Target Crypto-Asset, does the Provider have a system in which multiple persons in charge are involved in the transfer in accordance with procedures prescribed in advance in internal rules, etc.?

(B) Does the Crypto-Asset Exchange Service Provider manage the secret keys, etc. in a way that they cannot be used (signed) by anyone other than the authorized personnel? In particular, in cases where the secret keys, etc. are managed by physical media such as hardware or paper, are they stored in an environment that cannot be accessed by anyone

other than the authorized personnel, such as in a locked security room or a safety box?

(C) Has the Crypto-Asset Exchange Service Provider taken appropriate measures for the transfer of a Target Crypto-Asset, such as requiring an electronic signature using multiple secret keys, etc.? In cases where multiple secret keys, etc. are used, does the Crypto-Asset Exchange Service Provider manage them separately in different storage locations for each secret key, etc.?

(D) When transferring a Target Crypto-Asset, does the Crypto-Asset Exchange Service Provider confirm that the transaction details pertaining to the transfer of the Target Crypto-Asset are authentic?

(E) In cases where a Crypto-Asset Exchange Service Provider uses a mechanism in which Target Crypto-Assets are automatically transferred to the outside at the request of a user, has the Provider set the upper limit of the Target Crypto-Assets that can be transferred at one time or in a short time set?

(F) Has the Crypto-Asset Exchange Service Provider made backups in case the secret keys, etc. are lost? Does the Crypto-Asset Exchange Service Provider also manage such backups safely based on II-2-2-3-2 (3) (v) and (vi) as well as (B) above?

(G) Does the Crypto-Asset Exchange Service Provider make the transfer procedure of the Target Crypto-Assets subject to internal audit?

(4) Response in case of the leakage

(i) Has the Crypto-Asset Exchange Service Provider established an IT monitoring system capable of immediately detecting any leakage of a Target Crypto-Asset as well as other internal control systems necessary for immediately detecting such leakage?

(ii) Has the Crypto-Asset Exchange Service Provider established an internal communication system to ensure that, in the case of detecting the leakage of a Target Crypto-Asset, the detected details are communicated to the management team promptly and with certainty.?

(iii) With regard to the response in the case of detecting the leakage of a Target Crypto-Asset, has the Crypto-Asset Exchange Service Provider formulated a contingency plan that assumes the event of Target Crypto-Asset leakage and constructed any emergency systems that include the following measures for example?

(A) Measures necessary to prevent secondary damage

Note: For example, in cases where secret keys, etc. are stored in an environment connected to the Internet, the Crypto-Asset Exchange Service Provider is required to consider necessary measures, according to the leakage situation and the characteristics of the stored Crypto-Assets, such as by isolating the secret keys, etc. immediately from the Internet; transferring the Crypto-Assets that are managed with such secret keys, etc. immediately to an environment that is not connected to the Internet; and checking whether other Crypto-Assets are affected.

(B) Responses to the affected users (including the establishment of a consultation desk and the like)

Note: In recovering from damage to users, it should be noted that measures must be taken in accordance with the policy on performance of obligations set forth in Article 23(3) of the Cabinet Office Order.

(C) Reporting to and cooperation with the supervisory authorities, outsourced contractors, and other relevant parties

(D) Prompt cause analysis and consideration and implementation of new risk reduction

measures

Note: It should be noted that preconditions for a prompt cause analysis are to appropriately preserve evidence on relevant servers, etc., and to record access logs, etc., that contain sufficient information to track events.

II-2-2-5 Books and Documents

II-2-2-5-1 Purpose and Significance

Books and documents related to the Crypto-Asset Exchange Services are not only required to accurately reflect the business status of Crypto-Asset Exchange Service Providers and the Users' Property management status, but are also required to include the recording of Separate Management Audits results, thereby contributing to user protection. For this reason, laws and regulations stipulate the obligation to prepare and preserve such books and documents. In examining such books and documents, the following points shall be taken into consideration in light of the abovementioned intent.

II-2-2-5-2 Major Supervisory Viewpoints

(i) With regard to the preparation of books and documents, has the Crypto-Asset Exchange Service Provider developed a control environment necessary for the preparation of accurate books and documents, such as the establishment of internal rules, etc. that stipulate the purpose and use of books and documents, rather than simply enumerating the name of the books and the matters to be entered? In addition, has the Provider disseminated them company-wide through internal training, etc. so that its officers and employees properly handle cases in accordance with the internal rules, etc.?

Note: In cases where a transaction pertaining to the Crypto-Asset Exchange Services is contracted in a foreign currency, the money value must be entered in yen terms after the conversion into the Japanese currency, according to the Users' Property management method pertaining to the money. Conversion into the Japanese currency shall be made at the middle rate of the spot telegraphic transfer selling rate and the spot telegraphic transfer buying rate on the business day on which the amount of money of the user is calculated. Further, the source of such middle rate shall be, in principle, a principal financial institution of the Crypto-Asset Exchange Service Provider, but if the Provider has been continuously using another reasonable source, such source may as well be allowed. When converting a Crypto-Asset into the Japanese currency, refer to "II-2-1-4-2 Major Supervisory Viewpoints (9)."

(ii) In preparing order slips, does the Crypto-Asset Exchange Service Provider take the following measures, for example, so that the history of orders from users or orders for its own transactions can be accurately grasped ex post facto?

- Enter details of the order into the computer at the same time as the order is received (or at the same time the order is placed in the case of its own transaction)
- Always be ready to respond promptly to an inquiry from each user
- Back up and save input data
- The relevant system should automatically record the input time.
- In cases where input details are cancelled or corrected, the relevant system should keep the record of such cancellation or correction as it is.
- If it is impossible to prepare an order slip by directly inputting it into a computer at the same time as the order is received, because the order, which is for the next-day transaction, is

received after the computer system operation hours, or because the computer becomes unusable due to system down, etc., the order slip should be prepared by hand at the time of receiving the order. However, in cases where the Crypto-Asset Exchange Service Provider stores both the handwritten order slip prepared at the time of receiving the order and the computer-generated order slip later prepared with the execution result, etc. thereon together, no additional writing on the handwritten order slip is required.

(iii) Does the Crypto-Asset Exchange Service Provider have a framework that enables it to promptly ascertain and restore the amount of money and that of Crypto-Assets by each user in the event of any damage to the books and documents, including those backups?

(iv) Does any department, such as the Internal Audit Department, other than the books-and-documents-preparation division, verify the accuracy of the description of the books and documents?

II-2-2-6 Control Environments for Management of User Information

II-2-2-6-1 Purpose and Significance

Information regarding individual users of Crypto-Assets needs to be handled in an appropriate manner in accordance with the provisions of Articles 13 to 15 of the Cabinet Office Order, as well as the Act on the Protection of Personal Information (Act No. 57 of 2003; hereinafter referred to as the "Personal Information Protection Act") as well as the Guidelines on the Act on the Protection of Personal Information (General rules) (Provision to foreign third parties), (Obligation to confirm and record at the time of provision to third parties), (Anonymized information) (hereinafter collectively referred to as the "Personal Information Protection Guidelines"), the Guidelines on the Protection of Personal Information in the Financial Sector (hereinafter referred to as the "Financial Sector Personal Information Protection Guidelines") and the Guidelines for Practical Affairs regarding Safety Control Measures specified in the Guidelines on the Protection of Personal Information in the Financial Sector (hereinafter referred to as the "Practical Guidelines").

In addition, personal information including credit card information (number and expiration date, etc.)(hereinafter referred to as "credit card information, etc.") needs to be strictly managed because secondary damage such as spoofed purchase via unauthorized use of such information may occur if it is leaked.

In light of the above, when supervising Crypto-Asset Exchange Service Providers, the following points, for example, shall be taken into consideration.

Note: With regard to the handling of personal information, note that there are some cases in which necessary measures should be taken according to the delegation of authority to the competent minister for the relevant business under the Act on the Protection of Personal Information as needed.

II-2-2-6-2 Major Supervisory Viewpoints

(1) Control environments for management of user information

(i) Does the management team of the Crypto-Asset Exchange Service Provider recognize the necessity and importance of ensuring the appropriateness of managing information of users? Has the Crypto-Asset Exchange Service Provider developed an internal control environment, such as establishing an organizational structure (including establishing appropriate checks between departments) and formulating internal rules to ensure the appropriate management of such information?

(ii) Has the Crypto-Asset Exchange Service Provider formulated a specific standard for the

handling of user information and communicated it to all officers and employees through the provision of training and other means? In particular, with regard to the transmission of such information to third parties, has the Crypto-Asset Exchange Service Provider established the handling standard after sufficient consideration to ensure that procedures are carried out in accordance with the provisions of the aforementioned laws and regulations, the Personal Information Protection Guidelines, the Financial Sector Personal Information Protection Guidelines, and the Practical Guidelines?

(iii) Has the Crypto-Asset Exchange Service Provider established frameworks necessary for examining the management status of user information in a timely and appropriate manner? Such frameworks include management of access to user information (such as preventing access rights assigned to certain people from being used by others), measures to prevent the misappropriation of user information by insiders, and a robust information management system that prevents unauthorized access from the outside.
Also, has the Crypto-Asset Exchange Service Provider taken appropriate measures for preventing wrongful acts utilizing user information, such as the dispersal of authority concentrated upon specific personnel and the enhancement of controls and checks over personnel who have broad powers?

(iv) Has the Crypto-Asset Exchange Service Provider established frameworks for appropriately reporting to responsible divisions when user information has been leaked, and notifying relevant users, reporting to the relevant authorities, and disclosing to public in a prompt and appropriate manner to prevent secondary damage?
Also, does the Crypto-Asset Exchange Service Provider analyze the causes of information leaks and implement measures designed to prevent recurrence? Furthermore, in light of incidents of information being leaked at other companies, does the Crypto-Asset Exchange Service Provider examine measures needed to prevent a similar incident from occurring at its organization?

(v) Does the Crypto-Asset Exchange Service Provider conduct audits covering the broad range of business operations handling user information by its independent Internal Audit Department on a periodic or as-needed basis?
Also, has the Crypto-Asset Exchange Service Provider implemented appropriate measures, such as training programs, in order to increase the specialization of the staff engaged in audits pertaining to the management of user information?

(vi) Does the Crypto-Asset Exchange Service Provider regularly have its officers and employees participate in training sponsored by the Association or equivalent training in order to ensure the appropriate handling of information?

(2) Management of personal information

(i) With regard to information concerning individual users, has the Crypto-Asset Exchange Service Provider implemented the following necessary and appropriate measures for its safe management and supervision of persons in charge in order to prevent such information from being leaked, lost, or damaged, in accordance with Article 14 of the Cabinet Office Order?
(Necessary and appropriate measures concerning safety management)
(A) Measures based on Article 8 of the Financial Sector Personal Information Protection Guidelines
(B) Measures based on I, and Appendix 2 of the Practical Guidelines
(Necessary and appropriate measures concerning supervision of persons in charge)

(C) Measures based on Article 9 of the Financial Sector Personal Information Protection Guidelines

(D) Measures based on II of the Practice Guidelines

(ii) Has the Crypto-Asset Exchange Service Provider implemented measures to ensure that information regarding the race, religious beliefs, family origin, registered domicile, healthcare or criminal records of individual users, as well as other specified non-disclosure information (Note), are not used except for the cases specified in each item under Article 5(1) of the Financial Sector Personal Information Protection Guidelines?

Note: Other specified non-disclosure information includes the following;

(A) Information regarding labor union membership

(B) Information regarding ethnicity

(C) Information regarding sexual orientation

(D) Information regarding matters set forth in Article 2(iv) of the Enforcement Order of the Act on Protection of Personal Information

(E) Information regarding matters set forth in Article 2(v) of the Enforcement Order of the Act on Protection of Personal Information

(F) Information regarding facts that he/she has suffered damage by crime

(G) Information regarding social status

(iii) For credit card information, etc., has the Funds Transfer Service Provider implemented the following measures?

(A) Has the Crypto-Asset Exchange Service Provider set an appropriate period of time for keeping credit card information, etc., which takes into account the purpose of use and other circumstances? Does it limit the locations where such information is kept, and dispose of the information in a prompt and appropriate manner after the retention period has lapsed?

(B) Has the Crypto-Asset Exchange Service Provider implemented appropriate measures when displaying credit card information, etc. on computer monitors, such as not displaying whole credit card numbers, unless needed for business operations?

(C) Does the independent Internal Audit Department of the Crypto-Asset Exchange Service Provider conduct internal audit on a periodic or as-needed basis on whether the rules and systems for protecting credit card information, etc. are functioning effectively?

(iv) Has the Crypto-Asset Exchange Service Provider taken measures to comply with Article 12 of the Financial Sector Personal Information Protection Guidelines and other applicable provisions with regard to the provision of personal data to third parties? In particular, does the Crypto-Asset Exchange Service Provider obtain consents from individual users while paying attention to the following points according to the nature and methods of the business?

(A) When obtaining a consent from an individual user for the provision of his/her information to a third party in a non-face-to-face manner such as via PC or smartphone, etc., has the Crypto-Asset Exchange Service Provider designed the relevant webpage so that individual customers can easily understand the content and purpose of use of information provided to such third party by making it more customer-friendly in terms of the text of consent, letter size, screen specifications, manner of giving consent, etc. in accordance with Article 3 of the Financial Sector Personal Information Protection Guidelines?

(B) Even in the case where the Crypto-Asset Exchange Service Provider has obtained a consent for the provision of personal information to a third party from an individual user in the past, if the third party to which the information is provided or the content of information to be provided is different from the past case, or if the scope of provision of

such information exceeds the necessary extent to achieve a utilization purpose specified before, does the Crypto-Asset Exchange Service Provider obtain a consent from such individual user again?

(C) In cases where personal information of individual users is provided to multiple third party contractors or where the purpose of use of personal information varies at each third party contractor, does the Crypto-Asset Exchange Service Provider consider the scope of the third parties for which a consent of the user must be obtained, and how and when to obtain such consent in proper manner so that the individual users are able to understand the fact that their information shall be provided to multiple third parties, as well as the purpose of use at each third party contractor?

(D) In obtaining a consent for the provision of personal information to third parties, is the Crypto-Asset Exchange Service Provider mindful not to cause any risk of abuse of superior position or conflict on interests between it and the individual user? For example, is an individual user forced to give a consent beyond the reasonable scope of provision in terms of the third parties to which the personal information is provided, the purpose of use, or the content of information to be provided?

II-2-2-7 Dealing with Complaints (including Financial ADR System)

II-2-2-7-1 Purpose and Significance

In terms of user protection, one of the important activities for Crypto-Asset Exchange Service Providers is to sincerely respond to consultations, complaints, disputes, etc. (hereinafter referred to as "complaints, etc.") from users so as to get their understanding that such effort has the meaning of supplementing their accountability to users ex post facto.

In recent years, the importance of dealing with complaints, etc. ex post facto has been further increasing from the viewpoint of protecting users and ensuring the reliability of Crypto-Asset Exchange Business (which refers to Crypto-Asset Exchange Business as defined in Article 2(15) of the Act; the same shall apply hereinafter).

Based on these perspectives, a financial ADR system has been introduced as a framework for simply and expeditiously processing complaints and resolving disputes (refer to Note for description of ADR), and Crypto-Asset Exchange Service Providers are required to appropriately handle complaints, etc. taking into account this financial ADR system.

Note: ADR (Alternative Dispute Resolution)

An alternative method to litigation for resolving disputes which is based on agreement by the parties, such as mediation or arbitration. ADR is expected to result in prompt, simple, and flexible dispute resolution in a manner suited to the nature of the case, the circumstances of the parties, and so on.

In addition to consultations, there may be various forms of allegations regarding Crypto-Asset Exchange Business, including representation of dissatisfaction, such as so-called complaints and disputes, from users. It is important for Crypto-Asset Exchange Service Providers to appropriately deal with these various forms of allegations, and they are required to develop an appropriate internal control environment to enable such responses.

In addition, Crypto-Asset Exchange Service Providers are also required to develop appropriate control environments respectively for complaints and disputes in the financial ADR system.

However, it must be added that the distinction between these complaints and disputes is relative and they are connected with each other. In particular, in light of the requirement in the financial ADR system for designated ADR bodies (Note 1) to ensure links between complaint processing procedures

and dispute resolution procedures, rather than dealing with individual cases by formally dividing allegations made by users into "complaints" and "disputes," it is important that Crypto-Asset Exchange Service Providers deal with complaints and dispute appropriately while taking into consideration their relativity and connections.

Note 1: Designated ADR bodies refer to Designated Dispute Resolution Organizations for Crypto-Asset Exchange Business ("Designated Dispute Resolution Organizations" as defined in Article 2(13) of the Act, for which the category of Dispute Resolution Services is Crypto-Asset Exchange Business).

Note 2: It should also be kept in mind that an individual dispute that arises between a user and a Crypto-Asset Exchange Service Provider is, in general, a problem pertaining to a private-law contract, and as such, is basically a matter to be resolved between the parties via ADR or other judicial or legal proceedings.

II-2-2-7-2 Major Supervisory Viewpoints

The supervisors shall examine the respective internal control environments of Crypto-Asset Exchange Service Providers to grasp how they deal with complaints, etc., by paying attention to the following points, for example.

(i) Establishment of an internal control environment by the management team

Does the management team exercise its functions properly with regard to the establishment of the company-wide internal control environment for the function of dealing with complaints, etc.?

(ii) Development, dissemination, and thorough implementation of internal rules, etc.

(A) Has the Crypto-Asset Exchange Service Provider specified the divisions in charge of complaints, etc., their responsibilities and authorities, as well as the procedures for dealing with complaints, etc. in its internal rules, etc. so that complaints, etc. can be responded to and dealt with in a prompt, fair, and appropriate manner? In addition, has the Provider established procedures concerning business improvement so that the views of users are reflected in the conduct of business operations?

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment to disseminate internal rules, etc. to its officers and employees and thoroughly implemented them by means of training and other measures (including the distribution of manuals and so forth) so that business operations for dealing with complaints, etc. can be conducted based on those internal rules, etc.?

Particularly in cases where complaints, etc. are being made frequently by users, does the Crypto-Asset Exchange Service Provider first confirm how internal rules, etc. (not only those for dealing with complaints, etc.) are publicized and enforced at branches? And then does the Crypto-Asset Exchange Service Provider examine the causes and problem areas in terms of control environments?

(iii) Control environment for dealing with complaints, etc.

(A) Has the Crypto-Asset Exchange Service Provider appropriately appointed staff in charge of dealing with complaints, etc.?

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein relevant divisions cooperate and promptly deal with complaints, etc. from users? In particular, has the Crypto-Asset Exchange Service Provider developed a control environment wherein the responsible division or person in charge of dealing with complaints, etc. strives to fully understand user complaints, etc. faced by individual

employees, and reports promptly to the relevant divisions?

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it promptly settles any outstanding cases and prevents the occurrence of any long-term outstanding cases by conducting progress management aimed at the resolution of such complaints?

(D) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it improves the response provided at contact points according to the occurrence of complaints, etc., and wherein it can receive complaints, etc. extensively, such as by setting access hours and means of access (for example, multiple channels such as e-mail, telephone, and facsimile) that are considerate of user convenience? Also, has the Crypto-Asset Exchange Service Provider developed a control environment wherein it extensively publicizes these contact points and ways of making allegations, and wherein it makes them well known to users in an easy-to-understand manner taking into account their diversity?

(E) In dealing with complaints, etc., has the Crypto-Asset Exchange Service Provider developed a control environment for ensuring the proper handling of personal information in accordance with the Act on the Protection of Personal Information and other applicable laws and regulations, the Personal Information Protection Guidelines, etc.? (See "II-2-2-6 Control Environments for Management of User Information.")

(F) With regard to complaints, etc. concerning outsourced business operations conducted by an outsourced contractor, has the Crypto-Asset Exchange Service Provider developed a control environment for handling such complaints, etc. promptly and appropriately, such as by establishing a system of direct communication to the Provider itself (see "II-2-3-3 Outsourcing")?

(G) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it can communicate quickly with relevant divisions and cooperate with the police and other relevant organizations where necessary, in order to distinguish any pressure by anti-social forces disguised as complaints, etc. from ordinary complaints, etc. and to take a resolute stance against them?

(iv) Responses to users

(A) Does the Crypto-Asset Exchange Service Provider go beyond perceiving the dealing with such complaints, etc. as a simple problem of processing procedures, and instead regard it as a question of a control environment for providing ex post facto explanations and aim to resolve complaints, etc. with the understanding and agreement of each user wherever possible while suitably interviewing the respective users on the circumstances according to the nature of complaints, etc.?

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it provides users who have made complaints, etc. with appropriate explanations, as necessary, according to the progress of the procedures for dealing with complaints, etc. while also being considerate of the specific characteristics of the respective users, from the time complaints, etc. are made to after their settlement (for example, an explanation of the procedures for dealing with complaints, etc., notification to the effect that the allegation has been received, an explanation on the progress, an explanation of the results, etc.)?

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it not only deals with such complaints, etc. on its own but also refers the relevant users to appropriate external organizations (including the external organization that the Crypto-Asset Exchange Service Provider uses under the financial ADR system; the same

shall apply hereinafter), according to details of complaints, etc. and user requests, etc.? In addition, has the Provider developed a control environment wherein it provides information, such as the outline of its standard procedures? In cases where there is more than one means of processing a complaint or resolving a dispute (including the financial ADR system), users should be able to choose freely, and so in referring users to external organizations, care should be taken so that each user's choice is not unduly restricted.

(D) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, even during a period when proceedings for dealing with one of complaints, etc. are pending at an external organization, the Provider takes appropriate action where necessary with respect to the user who is the other party to said proceedings (such as ordinarily providing the user with general materials or explanations)?

(v) Information sharing, business improvements, etc.

(A) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein the complaints, etc. categorized into typical patterns and their respective results, etc. are reported to the Internal Control Department and the Sales Division, and wherein information necessary for the particular case is shared between those concerned, such as promptly reporting cases that are recognized as important to the Audit Department and the management team?

(B) Does the Crypto-Asset Exchange Service Provider properly and accurately record and store information on the contents of complaints, etc., and the results of dealing with them, including both complaints, etc. it deals with on its own, and those dealt with through the mediation of an external organization? Also, has the Crypto-Asset Exchange Service Provider developed a control environment wherein it analyzes the contents of complaints, etc., and the result of dealing with them, taking into consideration information, etc., provided by a designated ADR body, and applies this on an ongoing basis to the improvement of control environments for dealing with users and conducting administrative processes and to the formulation of measures for preventing any occurrence or recurrence of such complaints, etc.?

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein the internal checks and balances functions, such as those of inspection and audit, can function properly to ensure the effectiveness of how complaints, etc. are dealt with?

(D) In reflecting the results of dealing with complaints, etc. in the conduct of business operations, has the Crypto-Asset Exchange Service Provider developed a control environment wherein the management team supervises over any decisions to implement necessary measures for business improvement or recurrence prevention, as well as any examination and ongoing review of how the control environment for dealing with complaints, etc. should be?

(vi) Relationship with external organizations

(A) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it cooperates appropriately with external organizations in working toward the prompt resolution of complaints, etc.?

(B) In filing a petition for dispute resolution procedures for itself, has the Crypto-Asset Exchange Service Provider developed a control environment wherein it first responds sufficiently to the allegation of complaint, etc. from the user and goes through an appropriate internal deliberation on the need for the petition, rather than simply filing a petition without fully exhausting its own procedures?

II-2-2-7-3 Responses to the Financial ADR System

II-2-2-7-3-1 Major Supervisory Viewpoints in Cases Where a Designated Dispute Resolution Organizations for Crypto-Asset Exchange Business (a Designated ADR Body) Exists

In order to enhance user protection and improve user confidence in the Crypto-Asset Exchange Services, it is important to ensure substantial equality between Crypto-Asset Exchange Service Providers and users, and to resolve users' complaints, etc. in a neutral, fair, and effective manner. Therefore, in the financial ADR system, complaint processing and dispute resolution from a third-person perspective are conducted by designated ADR bodies with the participation of experts and others.

Under the financial ADR system, responses to complaint processing and dispute resolution are primarily regulated according to basic contracts for execution of procedures (Article 99(1)(viii) of the Act) concluded between Crypto-Asset Exchange Service Providers and designated ADR bodies.

Crypto-Asset Exchange Service Providers are required to appropriately address their obligations, etc. set forth in their basic contracts for execution of procedures, while bearing in mind the objective of processing complaints or resolving disputes at designated ADR bodies.

The supervisors shall examine how Crypto-Asset Exchange Service Providers respond to the financial ADR system, by paying attention to the following points, for example.

Note: In cases where there is a designated ADR body, even if a Crypto-Asset Exchange Service Provider is found to be in breach or negligence of the obligation to comply with procedures, this is the Crypto-Asset Exchange Service Provider's nonfulfillment pertaining to the basic contract for execution of procedures with the ADR body and does not immediately result in administrative disposition. Being mindful of this, the supervisory authorities should make a relevant judgment by overseeing the Crypto-Asset Exchange Service Provider's responses comprehensively and continuously.

(i) Basic contract for execution of procedures

(A) Has the Crypto-Asset Exchange Service Provider promptly concluded a basic contract for execution of procedures with a designated ADR body with regard to the Crypto-Asset Exchange Business it conducts?

For example, even if there are changes such as a designated ADR body having its designation rescinded or a new ADR body being designated, does the Crypto-Asset Exchange Service Provider select the best measure from the perspective of user convenience and promptly implement any necessary measures (such as implementing new complaint processing measures or dispute resolution measures, or concluding a new basic contract for execution of procedures)? Also, does the Crypto-Asset Exchange Service Provider take appropriate action, such as making it known to all users?

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment to faithfully perform the basic contract for execution of procedures concluded with a designated ADR body?

(ii) Publication, dissemination, and response to users

(A) Has the Crypto-Asset Exchange Service Provider properly publicized the name or trade name and the contact address of a designated ADR body with which the Crypto-Asset Exchange Service Provider has concluded a basic contract for execution of procedures? With regard to methods of publication, Crypto-Asset Exchange Service Providers are required to take measures suitable to the size and specific characteristics of their business

operations, such as presenting information on their websites, putting up posters at their branches, producing and distributing pamphlets, and conducting publicity activities through the mass media. Even supposing that a Crypto-Asset Exchange Service Provider has posted information on its website, if it is assumed that there are users who cannot view this information, the Crypto-Asset Exchange Service Provider is required to give consideration to these kinds of users.

In publicizing such information, does the Crypto-Asset Exchange Service Provider present it in a manner that is easy for users to understand? (For example, in the case of publicizing information on a website, the page should be so designed that users can easily access the page that provides information on the use of the financial ADR system.)

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it disseminates any necessary information to users, such as the flow of standard procedures by the designated ADR body and the effects of using a designated ADR body (such as the effect of interruption of prescription), in light of the basic contract for execution of procedures?

(iii) Complaint processing procedures and dispute resolution procedures

(A) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it receives a request from a designated ADR body for compliance with procedures, submission of materials, or the like, it responds to the request promptly, unless there is a justifiable reason not to do so?

(B) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it refuses a request from a designated ADR body to comply with procedures, submit materials, or the like, the Crypto-Asset Exchange Service Provider conducts a proper examination as an organization with respect to such decision of refusal, rather than the division that caused the complaint or dispute simply deciding by itself to refuse the request? Also, has the Crypto-Asset Exchange Service Provider developed a control environment wherein, wherever possible, it explains the reasons (justifiable reasons) for that decision?

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it is presented with a recommendation to accept a reconciliation plan or with a special conciliation proposal from a dispute resolution committee member, it makes prompt decisions on whether or not to accept it?

(D) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it has accepted a reconciliation plan or a special conciliation proposal, the division in charge takes prompt action, and the Inspection/Audit Department(s) conduct(s) a follow-up examination on matters including the progress of its fulfillment?

(E) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it rejects acceptance of a reconciliation plan or a special conciliation proposal, it promptly explains its reasoning and takes necessary action, such as instituting legal proceedings, in light of the operational rules (which refer to the "operational rules" as defined in Article 52-67(1) of the Banking Act, which shall be applied mutatis mutandis pursuant to Article 101 of the Act)?

II-2-2-7-3-2 Major Supervisory Viewpoints in Cases without Designated Dispute Resolution Organizations for Crypto-Asset Exchange Business (Designated ADR Bodies)

In the financial ADR system, even in cases where there is no designated ADR body, there is a legal requirement for Crypto-Asset Exchange Service Providers to instead implement complaint processing measures and dispute resolution measures. Crypto-Asset Exchange Service Providers are required to ensure complete user protection and to strive to improve user confidence by implementing these measures properly and by resolving any complaints or disputes regarding Crypto-Asset Exchange Business in a simple and expeditious manner.

The supervisors shall examine cases where Crypto-Asset Exchange Service Providers implement complaint processing measures and dispute resolution measures by paying attention to the following points, for example.

(i) Selection of complaint processing measures and dispute resolution measures

Does the Crypto-Asset Exchange Service Provider, in view of the nature of its Crypto-Asset Exchange Business, the occurrence of complaints, etc., its trading area, and other factors, appropriately select one or more of the following measures prescribed by laws and regulations as its complaint processing measures or dispute resolution measures? In such cases, it is desirable that the Crypto-Asset Exchange Service Provider, in doing so, should have measures in place that enhance convenience for the user in making complaints or disputes, such as providing an environment that makes it easier for the user to access relevant services in terms of geography.

(A) Complaint processing measures

a) Have consumer counselors or the like with certain experience provide advice and guidance to employees engaged in complaint processing;
b) Establish and publicize its own business management system and internal rules;
c) Use the Association;
d) Use the National Consumer Affairs Center of Japan or a local consumer affairs center;
e) Use a designated ADR body for another business category; and
f) Use a corporation capable of fairly and appropriately executing complaint processing services.

(B) Dispute resolution measures

a) Use the certified dispute resolution procedures set forth in the Act on Promotion of Use of Alternative Dispute Resolution;
b) Use a bar association;
c) Use the National Consumer Affairs Center of Japan or a local consumer affairs center;
d) Use a designated ADR body for another business category; and
e) Use a corporation capable of fairly and appropriately executing dispute resolution services.

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it continuously monitors the processing status of complaints and disputes, and where necessary, reviews and revises its complaint processing measures and dispute resolution measures?

(D) In cases where the Crypto-Asset Exchange Service Provider utilizes a corporation that can conduct complaint processing services or dispute resolution services in a fair and appropriate manner ((A)f or (B)e above), does the Crypto-Asset Exchange Service Provider assess whether said corporation is a corporation who has a financial basis and personnel structure that are sufficient to fairly and appropriately carry out operations pertaining to the complaint processing and dispute resolution(Article 32(1)(v) and (2)(iv) of the Cabinet Office Order), in a reasonable manner based on considerable materials and

other factors?

(E) In cases where the Crypto-Asset Exchange Service Provider utilizes an external organization, although it is not a requirement for the Crypto-Asset Exchange Service Provider to necessarily enter an outsourcing contract, etc. with said external organization, it is desirable to make arrangements in advance regarding matters such as the flow of standard procedures and terms and conditions regarding the burden of expenses.

(F) With regard to cases where expenses arise when the procedures of an external organization are used, has the Crypto-Asset Exchange Service Provider taken measures to prevent the expenses from becoming an impediment to the filing of a petition for complaint processing or dispute resolution, such as taking measures likely to prevent the user's share of expenses from becoming excessive?

(ii) Operation

The supervisory authorities shall examine whether the Crypto-Asset Exchange Service Provider has made inappropriate use of the complaint processing measures and dispute resolution measures, such as limiting the scope of application excessively. It should also be kept in mind whether the Crypto-Asset Exchange Service Provider has maintained appropriate coordination between complaint processing measures and dispute resolution measures.

(iii) Points to note regarding complaint processing measures (in cases where Crypto-Asset Exchange Service Providers develop their own control environments)

(A) Cases where a control environment is developed wherein consumer counselors or the like give guidance and advice to employees

a) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it improves the skills of its employees engaged in processing complaints, such as periodically conducting a training run by consumer counselors or the like?

b) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein it utilizes the specialized knowledge and experience of consumer counselors and the like, where necessary, for processing individual cases, such as building a network with consumer counselors and the like?

(B) Cases where a Crypto-Asset Exchange Service Provider develops its own operational system and internal rules

a) Has the Crypto-Asset Exchange Service Provider properly developed an operational system and internal rules according to the status of occurrence of complaints? And has it developed a control environment wherein it processes complaints in a fair and appropriate manner based on said system and rules?

b) Has the Crypto-Asset Exchange Service Provider made users aware of the contact point for making complaints in an appropriate manner? And has it properly published the operational system and internal rules pertaining to complaint processing? In terms of the content of the dissemination and publications, although publishing the full text of the internal rules is not necessarily needed, in order for users to confirm for themselves whether complaints are being processed in accordance with appropriate procedures, it is important that the contact for inquiry about the complaint processing and the flow of standard operations be clearly indicated. In light of this, the supervisors should check whether the Crypto-Asset Exchange Service Provider has published the information covering these matters. For the methods of publicity and publication, refer to II-2-2-7-3-1(ii).

(iv) Points to note regarding complaint processing measures (when using external organizations) and dispute resolution measures

(A) In cases where a Crypto-Asset Exchange Service Provider is using an external organization, from the perspective of user protection, it is desirable that the Crypto-Asset Exchange Service Provider disseminate and publish information on the external organization, including, for example, the fact that users are eligible to use the external organization for making complaints or disputes, the name of the external organization, its contact information, instructions on how to use it, and so forth, in a manner that is easy for users to understand.

(B) If the petition for complaint processing or dispute resolution is outside the scope handled by the external organization to which the user was first referred by the Crypto-Asset Exchange Service Provider because of geographical reasons, the nature of the complaint or dispute, or for any other reason, or if the petition is suitable for handling by another external organization, etc. (not limited to external organizations used by the Crypto-Asset Exchange Service Provider as complaint processing measures or dispute resolution measures), has the Crypto-Asset Exchange Service Provider developed a control environment for referring users to other external organizations?

(C) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it receives a request from an external organization for compliance with complaint processing or dispute resolution procedures, a request for an investigation of the facts, a request for the submission of relevant materials, or the like, it responds to the request promptly in light of the rules, etc. of the external organization?

(D) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it refuses a request for compliance with complaint processing or dispute resolution procedures, a request for an investigation of the facts, a request for the provision of relevant materials or the like, the Crypto-Asset Exchange Service Provider conducts a proper examination as an organization with respect to such decision of refusal, in light of the details of the complaint or dispute, the nature of the facts or materials, and the rules, etc. of external organizations, rather than the division that caused the complaint or dispute simply deciding by itself to refuse the request? Also, has the Crypto-Asset Exchange Service Provider developed a control environment wherein it explains the reasons for the refusal wherever possible in light of the rules, etc. of the external organization?

(E) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it is presented with a proposed solution such as a reconciliation plan or mediation plan from an external organization that has commenced dispute resolution procedures (hereinafter referred to as a “proposed solution”), it makes prompt decisions on whether or not to accept the proposed solution, in light of the rules, etc. of the external organization?

(F) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it has accepted a proposed solution, the division in charge takes prompt action, and the Inspection/Audit Department(s) conduct(s) a follow-up examination on matters, including the progress of its fulfillment?

(G) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein, in cases where it rejects acceptance of a proposed solution, it promptly explains its reasoning and takes necessary action, in light of the rules, etc. of the external

organization?

II-2-2-7-4 Provision of Information to Users

Under laws and regulations, Crypto-Asset Exchange Service Providers are required to clearly indicate how they respond to the financial ADR system as information to users. When providing such information, in cases where there is no designated ADR body, Crypto-Asset Exchange Service Providers are required to explain the details of their complaint processing measures and dispute resolution measures. In addition to this, it should be kept in mind that Crypto-Asset Exchange Service Providers need to explain relevant information in the context of their actual situation such as, if, for example, a Crypto-Asset Exchange Service Provider utilizes an external organization, the name and point of contact thereof, etc. (in cases where part of the services pertaining to the complaint processing or dispute resolution are entrusted to another organization, then including such other organization).

II-2-2-8 Response to ICO

II-2-2-8-1 Purpose and Significance

Although without a clear definition, an Initial Coin Offering (ICO) in general collectively means an activity to procure legal tender or Crypto-Assets from the public using a digital token issued by a company or other entity. In cases where a token issued through an ICO falls under the category of Crypto-Assets as defined in Article 2(5) of the Act, the act of selling or exchanging the token for another Crypto-Asset as its business (hereinafter referred to as "sales" or "sell" in II-2-2-8) falls under the category of the Crypto-Asset Exchange Services.

Note 1: However, if a Crypto-Asset Exchange Service Provider sells a token at the request of the issuer of the token, and the issuer does not sell the token at all, the issuer's act is not considered to be basically applicable to the Crypto-Asset Exchange Services.

It should be noted that the applicability of the issuer's act to the Crypto-Asset Exchange Services shall be ultimately determined individually and specifically, after taking into consideration the content of the contract between the issuer and the Crypto-Asset Exchange Service Provider, the content of the sales activities, the degree of the issuer's involvement in the sales, and so on,

Note 2: It should be noted that in cases where an ICO has the nature of an investment, such as the right of the token issuer to receive a distribution of future business profits, etc., is indicated on the token, the token is subject to the Financial Instruments and Exchange Act and is not subject to the Act.

Such an act is intended to raise funds through the sales of the token, but there may be cases where user protection is not sufficiently ensured, such as the occurrence of fraudulent cases or sloppily planned cases due to unclear contents of the rights of the token holder, failure to screen the feasibility of the project for which the funds are raised (hereinafter referred to as the "Target Project"), or failure to disclose necessary information.

In light of the above, when supervising Crypto-Asset Exchange Service Providers who sell these tokens, the supervisory authorities shall request the Crypto-Asset Exchange Service Providers to report the sales status of the tokens on a regular or as-needed basis in order to confirm whether the user protection and the appropriateness of their business are fully ensured. The supervisory authorities should also pay particular attention to the following points in light of the self-regulatory rules of the Japan Virtual and Crypto assets Exchange Association "Rules on Sales of New Crypto-Assets."

II-2-2-8-2 Major Supervisory Viewpoints

(1) Cases where the issuer sells the token on its own

(i) Does the issuer properly examine and verify the eligibility and feasibility of the Target Project, as well as the appropriateness of the token it handles?

(ii) Does the issuer provide customers with information on the issuer, the existence or non-existence and content of obligations owed to token holders, the basis for calculating the sales price of the token, the business plan document concerning the Target Project, and the feasibility of the Project, etc. when it sell the token?

Note: In providing information on the Target Project, the issuer should kept in mind that the objectivity and appropriateness of such information are required so that customers do not have unfounded expectations.

(iii) Does the issuer continuously or timely disclose, in an appropriate manner, the issuer's financial conditions, the sales status of the token, the progress status of the Target Project, and other matters that will affect the decision on the purchase and sale of the token, etc.?

(iv) Does the issuer manage the funds raised through the token sales separately from other funds and appropriately manage them, such as by not using them for purposes other than those disclosed to users in advance?

(v) Does the issuer verify the safety of each blockchain and smart contract used for the token, the wallet in which the token is stored and other systems that affect the quality of the token, and verify the safety of the systems on a regular or as needed basis, even after the token sales?

(vi) Does the issuer examine the appropriateness of the sales price in advance in order to prevent the token being sold in extremely inappropriate conditions in terms of the quantity, the price, and so on?

(2) Cases where a Crypto-Asset Exchange Service Provider sells the token on behalf of the issuer

In cases where a Crypto-Asset Exchange Service Provider sells the token on behalf of the issuer, the supervisory authorities shall pay attention to the following points, in addition to (1)(i)), (ii), (v), and (vi) above.

(i) Has the Crypto-Asset Exchange Service Provider established appropriate rules concerning the examination of not only the eligibility and feasibility of the Target Project, and the appropriateness of the token it handles, but also the issuer's financial conditions and other matters that contribute to judging the appropriateness of the token sales? And then does the Provider conduct substantive examinations in a proper manner? In addition, has the Crypto-Asset Exchange Service Provider established a system that enables it to verify the results of such examinations?

(ii) Has the Crypto-Asset Exchange Service Provider established a system to appropriately conduct examinations, such as by ensuring the independence of the division in charge of such examinations from the sales department in terms of its functions and effects? Also, for selling the token, does it have a function to verify and evaluate conflicts of interest with other internal divisions? Moreover, based on such a function, has the Crypto-Asset Exchange Service Provider developed a control environment to appropriately prevent a situation where a conflict of interest arises?

(iii) Does the Crypto-Asset Exchange Service Provider conduct necessary monitoring to ensure appropriate information disclosure by the issuer? And has it established a system to allow users to easily access information disclosed by the issuer?

(iv) Does the Crypto-Asset Exchange Service Provider conduct necessary monitoring to ensure

appropriate management of the funds procured by the issuer?

(v) In addition to (iii) and (iv) above, does the Crypto-Asset Exchange Service Provider conduct necessary monitoring of the issuer so that necessary measures are taken to protect users? If the issuer has not taken necessary measures to protect users, does the Crypto-Asset Exchange Service Provider make sure to take appropriate measures, such as suspending the token sales? Does the contract with the issuer provide the authority necessary to take such measures?

II-2-3 Administrative Operations

II-2-3-1 IT System Risk Management

II-2-3-1-1 Purpose and Significance

Information technology (IT) system risk refers to the risk of loss incurred by a user or a Crypto-Asset Exchange Service Provider due to a computer system failure, malfunction, or other inadequacies, and/or the risk that a user or a Crypto-Asset Exchange Service Provide incurs a loss due to the unauthorized use of a computer. Because of the nature of their business, Crypto-Asset Exchange Service Providers often have sophisticated and complex information systems based on the Internet, and because Crypto-Assets have property value that can be electronically recorded in blockchains and transferred through networks, cyberattacks, which become increasingly sophisticated every day, pose the risk of unauthorized access to or leakage of important information. Therefore, in addition to regular risk evaluation, each Crypto-Asset Exchange Service Provider needs to grasp changes in the external environment, accidents, and incidents, and to evaluate risk in a timely manner such as by examining whether or not they affect its own systems. In particular, as external services (cloud, etc.) are often used, it is important to develop a control environment for outsourcing management. The safe and stable system operation is a major prerequisite for ensuring the reliability of the payment service system and Crypto-Asset Exchange Service Providers. It is extremely important to ensure the basic matters of system development and operation and to enhance and strengthen the overall control environment for managing IT system risk. To this end, each Crypto-Asset Exchange Service Provider needs to secure management resources, and the management team should take the initiative in such efforts as formulating IT strategies.

From these viewpoints, it is extremely important for the management team of a Crypto-Asset Exchange Service Provider to show leadership, link information technologies to management strategies and thereby have “IT governance,” which is a mechanism to create corporate value through such initiatives, work properly and well.

Reference: Summary of Issues and Practices for Dialogue on IT Governance of Financial Institutions (June 2019)

In this regard, however, even if a Crypto-Asset Exchange Service Provider fails to respond literally as described in each of the following supervisory viewpoints, it shall not be regarded as inappropriate if it is deemed that there are no particular problems from the viewpoint of user protection in light of the scale and characteristics of such Crypto-Asset Exchange Service Provider.

II-2-3-1-2 Major Supervisory Viewpoints

(1) Recognition of IT system risk

(i) Have officers and employees, including the representative director, fully recognized the importance of IT system risk, and formulated a basic policy for the company-wide management of IT system risk?

Also, does the Crypto-Asset Exchange Service Provider review IT system risk regularly and revise the basic policy based on the results?

(ii) Does the Crypto-Asset Exchange Service Provider formulate an IT system strategy as part of its management strategy, and receive approval from the Board of Directors? It is desirable that such IT system strategy includes a medium- to long-term development plan.

(iii) Has the representative director recognized that prevention of an IT system failure and cybersecurity incident (hereinafter referred to as "IT system failures, etc.") and efforts for speedy recovery on the occurrence of such IT system failures, etc. is an important issue for the management, and developed an appropriate control environment?

Note: "Cybersecurity incidents" refer to instances of cybersecurity being threatened by so-called "cyberattacks", including unauthorized intrusion, theft, modification, and destruction of data, failure or malfunction of information systems, and execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

(iv) Does the Board of Directors appoint an officer who oversees and manages IT system, fully recognizing the importance of IT system risk? It is desirable that the officer in charge of IT systems should be a person who has sufficient knowledge and experience in IT systems to properly pursue the relevant operations.

(v) Has the Crypto-Asset Exchange Service Provider developed a control environment in which checks and balances are carried out, such as by having the IT System Risk Management Department monitor the IT Systems Department and by separating the person in charge of development from the person in charge of operation within the IT Systems Department?

(vi) Have the representative director and directors (or directors and executive officers in case where the Crypto-Asset Exchange Service Provider is a company with nominating committee, etc.) determined their specific responsibility to assume and response to take in case of crisis where an IT system failure, etc. occurs?

Also, do they conduct drills giving directions by themselves and ensure the effectiveness thereof?

(2) Control environment for managing IT system risk

(i) Has the Board of Directors established the risk management environment while fully understanding that, due to highly networked computer system, if risk becomes apparent, the impact would cause chain reaction, spread widely and seriously, and adversely affect the management of the Crypto-Asset Exchange Service Provider?

(ii) Has the Crypto-Asset Exchange Service Provider established the basic policy for managing IT system risk? Does the basic policy for managing the IT system risk contain the security policy (a basic policy for proper protection of information assets of an organization) and the policy on outsourced contractors?

(iii) Is the Crypto-Asset Exchange Service Provider basing the details of its control environment for managing the IT system risk on criteria that allow it to judge objective levels of its details?

Also, does the Crypto-Asset Exchange Service Provider revise, on a continual basis, its control environment for managing IT system risk according to identification and analysis of IT system failures, etc., results of implementation of risk management, progress of technology, etc.?

Note: It is desirable that such control environment for managing IT system risk is regularly evaluated by a third party (external organization).

(3) Assessment of IT system risk

(i) Does the IT Systems Department recognize and assess risks periodically and in a timely manner by recognizing that risks are becoming diversified due to changes in the external environment, such as seen in the examples of IT system failures, etc. induced by large-scale transactions as a result of increased user channels and efforts to enhance information networks that bring more diverse and broad-based impact?

In addition, does the Department take sufficient measures against identified risks, and then assess residual risks? Does it report such measures and assessment to the Board of Directors?

Does the IT system risk include the following?

- Risks arising from the use of external services
- Risks arising from the disclosure, provision, and connection of API

(ii) Do the department in charge of users cooperate with the IT Systems Department at the time of introduction of new services and/or at the time of any change in the content and method of any service? And does the IT Systems Department evaluate relevant IT systems regardless of whether the system is newly developed or not?

(4) Management of information security

(i) Has the Crypto-Asset Exchange Service Provider developed a policy, prepared organizational readiness, introduced internal rules, and developed an internal control environment in order to appropriately manage information assets? Also, is it making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies?

Note: Information assets refer to information itself and the information systems that handle it, including hardware, software, networks, etc. that make up the information systems.

(ii) Does the Crypto-Asset Exchange Service Provider manage information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity, and availability of information? Also, are the individuals responsible for information security tasked to handle the security of IT system, data, and network management?

(iii) Does the Crypto-Asset Exchange Service Provider take measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses?

Also, has the Crypto-Asset Exchange Service Provider implemented physical security measures for the locations where information assets are handled, according to the importance of the information assets?

(iv) Does the Crypto-Asset Exchange Service Provider comprehensively identify, grasp and manage important information for which it should be responsible?

Does the scope of important information to be identified by the Crypto-Asset Exchange Service Provider cover information and data used in the course of business operations or stored in IT systems and kept by outsourced contractors and include data, for example, as listed below?

- Data stored in the areas within the IT system that are not used in ordinary operations
- Data output from the IT system for analyzing system failures

(v) Does the Crypto-Asset Exchange Service Provider assess importance and risks regarding important information that has been identified?

Also, has it developed rules to manage information, such as those listed below, in

accordance with the importance and risks of each type of information?
- Rules to encrypt or mask information
- Rules for utilizing information
- Rules on handling data storage media, etc.

(vi) Has the Crypto-Asset Exchange Service Provider introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as those listed below, for important information?
- Provision of access rights limited to the extent necessary according to the respective roles of the utilization sites (including overseas ones)
- Provision of access rights limited to the extent necessary according to the authority of employees
- Storage and monitoring of access logs
- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, or system administrators and system users, etc.
- Separation of the production environment from the test environment for testing a system, etc.

(vii) Has the Crypto-Asset Exchange Service Provider introduced management rules, such as encryption and masking, for confidential information in particular among important information? Also, has it introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs, etc.?
Note that "confidential information" refers to any information that may cause damage or loss to users and/or the company itself if it is disclosed or stolen, such as encryption keys, PINs, passwords, credit card information, etc.

(viii) Does the Crypto-Asset Exchange Service Provider give due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, confidential information, and treat such information in a stricter manner?

(ix) Does the Crypto-Asset Exchange Service Provider periodically monitor its information assets to see whether they are managed properly according to management rules, etc., and review the control environment on an ongoing basis?

(x) Does the Crypto-Asset Exchange Service Provider conduct security education (including securities education at outsourced contractors) to all officers and employees in order to raise awareness of information security?

(5) Cyber security management

(i) Has the Board of Directors, etc. introduced the necessary control environment upon recognizing the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks?

(ii) Has the Crypto-Asset Exchange Service Provider introduced systems to maintain cybersecurity, such as those listed below, in addition to making the organization more secure and formulating internal rules?
- Monitoring systems against cyberattacks
- Systems to report cyberattacks and public-relation system when attacks occur
- Emergency measures by an in-house Computer Security Incident Response Team (CSIRT) and systems for early warning
- Systems of information collection and sharing through information-sharing organizations,

etc.

(iii) Has the Crypto-Asset Exchange Service Provider introduced a multi-layered defense system against cyberattacks that combines risk-based security measures respectively for inbound perimeter control, internal network security control, and outbound perimeter control?

- Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, unauthorized intrusion detection system, unauthorized intrusion prevention system, etc.);
- Internal measures (e.g. proper management of privileged IDs and passwords, deletion of unnecessary IDs, monitoring of execution of specific commands, securing of production systems (between servers) (packet filtering and encryption of communications), separation of networks in development environments (including test-phase environments) and use-phase environments, separation of network segments according to usage purposes, etc.)
- Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

(iv) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein the Provider promptly implements the following measures to prevent damage from expanding when cyberattacks occur?

- Identifying IP addresses of attackers, and blocking off attacks;
- Functions to automatically decentralize accesses against DDoS attacks; and
- Temporary suspension, etc. of the entire system or part thereof

Also, has the Crypto-Asset Exchange Service Provider prepared procedures for follow-up investigations (forensic investigations), such as log preservation and image copy acquisition, in order to confirm the scope of impact and determine the cause?

(v) Has the Crypto-Asset Exchange Service Provider clearly established and systematically implemented procedures for regularly collecting, analyzing, and responding to information on vulnerabilities as well as threat information?

In addition, are necessary measures introduced for vulnerabilities in the IT system, such as updating of the operating system and application of security patches, in a timely manner?

(vi) With regard to cybersecurity measures, does the Crypto-Asset Exchange Service Provider assess its security levels periodically, such as by using security assessment (vulnerability assessment, source code assessment, and penetration testing, etc.) by a third party (an external organization) and make efforts to improve its security measures?

Upon the occurrence of cybersecurity breaches in Japan and abroad, does the Crypto-Asset Exchange Service Provider assess the relevant risks in a timely and appropriate manner?

(vii) When conducting non-face-to-face transactions using the Internet and other means of communication, has the Crypto-Asset Exchange Service Provider introduced an appropriate authentication method that matches the risks of transactions, such as the following?

- Authentication methods that do not rely on fixed IDs/passwords, such as variable passwords and digital certificates
- Transaction authentication through multiple channels, such as by using, for example, a device that is different from a PC or a smartphone used for transactions; and
- Adoption of a trading password that is different from the login password, etc.

(viii) When conducting non-face-to-face transactions using the Internet and other means of communication, has the Crypto-Asset Exchange Service Provider taken following anti-fraud measures, for example, corresponding to the business?

- Interrupting communications from invalid IP addresses

- Taking measures to encourage users to introduce and update security software that allows them to detect and remove viruses, etc.
- Introduction of a system to detect unauthorized log-ins, abnormal transactions, etc. and promptly notify such anomalies to users; and
- Displaying the last login (logoff) date and time on the screen, etc.

(ix) Has the Crypto-Asset Exchange Service Provider developed contingency plans against potential cyberattacks? And does it conduct exercises and review such plans? Also, does it participate in industry-wide exercises as necessary?

(x) Has the Crypto-Asset Exchange Service Provider formulated plans to train and develop personnel responsible for cybersecurity and implemented them?

(6) IT system planning/development/management

(i) Does the Crypto-Asset Exchange Service Provider make continuous efforts to identify risks inherent in the current IT system and make investment in maintaining such efforts and eliminating risks in a planned manner?

(ii) Has the Crypto-Asset Exchange Service Provider formulated rules for creating documents and programs related to design and development in accordance with the IT system development process? In the IT system design/development stage, the following items related to security should be included.

- Clarifying specific security requirements
- Taking measures to prevent any vulnerability in the system such as secure coding

Also, has the Crypto-Asset Exchange Service Provider formulated rules concerning approval of the planning/development/transfer of development projects?

(iii) Does the Crypto-Asset Exchange Service Provider appoint and assign a responsible person to each IT system development project and manage the project according to the development plan?

(iv) Has the Crypto-Asset Exchange Service Provider formulated the rules and procedures for quality control that include the following?

- Reviewing and keeping records
- Formulating and evaluating the completion criteria for each process
- Making the performance design sufficient and managing the IT system capacity and the upper limit of performance
- Grasping the threshold limit during IT system development, etc.

(v) Has the Crypto-Asset Exchange Service Provider established rules concerning IT system changes? Also, are documents related to IT system changes prepared? Are they approved by the responsible person?

(vi) Has the Crypto-Asset Exchange Service Provider formulated the rules and procedures for IT system management, taking into account the following points?

- Mechanism to efficiently isolate a problem at the time of detection in the monitoring setting
- Unified escalation rules for monitoring
- Incorporating records, approvals, and inspections into the work process
- Recording and retaining in writing the implementation status of operations related to IT system management, etc.

(vii) Has the Crypto-Asset Exchange Service Provider established the purpose, policy, and scope of application of IT system configuration management?

Also, does it grasp the configuration in terms of the following points, and thereby confirm

the effectiveness of such management?

- Physical resources (hardware, networks, servers, PCs, etc.)
- Logical resources (licenses, software, connection configurations, etc.)
- Cloud services, outsourcing to third parties, etc.

(viii) In developing IT systems, does the Crypto-Asset Exchange Service Provider work out a test plan and conduct a test in an appropriate and sufficient manner, such as by involving the departments in charge of users in it?

(ix) Has the Crypto-Asset Exchange Service Provider secured personnel who are familiar with the mechanisms of the current IT system and have expertise in IT system planning, development, and operation management?

Has the Crypto-Asset Exchange Service Provider formulated a specific plan for the succession of the current IT system structure and development technology and the development of human resources with expertise, and implemented them?

(7) IT system audit

(i) Does the Internal Audit Department, which is independent from the IT Systems Department, conduct periodic IT system audits by personnel familiar with IT system matters?

Note: External audits may be used instead of internal audits if it is considered more effective to introduce IT system audits by external auditors.

(ii) Are the targets of IT system audits selected based on the assessed risks after the risk assessment of the entire operations?

(iii) Are the results of the IT system audit reported to the Board of Directors in a proper manner? Do the audited departments receive feedback from the Audit Department and make improvements according to the audit results?

(8) Outsourcing management

(i) Does the Crypto-Asset Exchange Service Provider, in selecting the outsourced contractors (including IT system-related subsidiaries), assess them based on selection criteria and give careful consideration?

(ii) When using external services such as cloud services, does the Crypto-Asset Exchange Service Provider examine risks associated with the services used and take necessary measures?

For example, does it implement the following measures?

- Processing critical data
- Grasping the storage sites and ensuring authority to audit them
- Reflecting the authority to monitor, etc. in the contract
- Obtaining and evaluating assurance reports, etc.

(iii) Does the Crypto-Asset Exchange Service Provider, in entering an outsourcing contract with an outsourced contractor, set out in the contract the division of roles and responsibilities with the outsourced contractor, audit authority, subcontracting procedures, level of services provided, etc.? Also, does the Crypto-Asset Exchange Service Provider present to the outsourced contractor rules that its officers and employees are required to adhere to and security requirements, as well as define them in the contract, etc.?

(iv) Is risk management carried out properly in outsourced IT system work (including multi-tiered outsourcing)?

In particular, in cases where the Crypto-Asset Exchange Service Provider outsources its IT system work to two or more contractors, related administrative work becomes complicated

and a higher level of risk management is required. In this context, has the Crypto-Asset Exchange Service Provider developed a control environment upon fully understanding such fact?

In cases where IT system-related administrative work is outsourced to contractors, too, does the Crypto-Asset Exchange Service Provider properly manage the risk thereof in the same manner as outsourcing of IT system work?

(v) Does the Crypto-Asset Exchange Service Provider, as an outsourcer, regularly check and monitor to confirm that outsourced work (including multi-tiered outsourcing) is carried out appropriately?

Also, does the Crypto-Asset Exchange Service Provider take necessary measures not to leave everything to outsourced contractors by, for example, placing its staff at an outsourced contractor's site to monitor the outsourced work, etc.?

In addition, does the Crypto-Asset Exchange Service Provider put in place a control environment that allows the Provider, as an outsourcer, to monitor and track the status of user data being processed at outsourced contractors?

(vi) Does the Crypto-Asset Exchange Service Provider audit its important outsourced contractors by its Internal Audit Department or IT system auditors, etc. and/or obtain any reports on internal control of outsourced contractors?

Reports deemed as "reports on internal control of outsourced contractors" refer to, for example, the IT Committee Practical Guidelines No. 7, the "assurance reports on internal control over security, availability, processing integrity, confidentiality, and privacy of entrusted services" published by the Japanese Institute of Certified Public Accountants (JICPA), or the Audit and Assurance Practice Committee Practical Guidelines No. 86, the "assurance report on internal control of entrusted business" (JICPA).

(9) Contingency plan

(i) Has the Crypto-Asset Exchange Service Provider formulated a contingency plan and prepared written procedures in line with the plan?

In addition, has the Provider established an emergency system that includes important outsourced contractors?

(ii) Is the Crypto-Asset Exchange Service Provider basing the details of its contingency plan on guides that allow it to judge objective levels of its details (such as "Manual for the Development of Contingency Plans in Financial Institutions (Plans for Measures in the Event of Emergencies)" compiled by the Center for Financial Industry Information Systems)?

(iii) When formulating a contingency plan, does the Crypto-Asset Exchange Service Provider assume not only contingencies due to natural disasters but also IT system failures, etc. due to internal or external factors?

Also, does the plan include sufficient risk scenarios assuming the following risks?

- Cyberattack
- Disaster and pandemic
- IT system failure
- Information leakage, etc.

(iv) Does the Crypto-Asset Exchange Service Provider review assumed scenarios in its contingency plan in a timely and appropriate manner by, for example, taking into consideration case studies of IT system failures, etc. at other Crypto-Asset Exchange Service Providers and results of deliberations at the Central Disaster Management Council, etc.?

(v) Does the Crypto-Asset Exchange Service Provider regularly conduct a drill based on its contingency plan?
Also, has the Provider established a framework for systematically reviewing and expanding its contingency plan based on such drill results?
It is desirable that drills based on the contingency plan are conducted at the company-wide level and jointly with outsourced contractors, etc.

(vi) Has the Crypto-Asset Exchange Service Provider introduced off-site backup IT systems, etc. in advance for important IT systems whose failure could seriously affect business operations? And has it developed a control environment to address disasters or IT system failures, etc. so that normal business operations can be speedily brought back?
Also, has the Crypto-Asset Exchange Service Provider taken measures in case of data loss, such as taking backup of data on a regular basis?

(10) Response to IT system failures

(i) Has the Crypto-Asset Exchange Service Provider developed a control environment, upon assuming a worst-case scenario in preparation for IT system failures, etc. to take necessary measures accordingly?
In addition, does it take measures to minimize the impact on users in the event of an IT system failure, etc.?

(ii) Has the Crypto-Asset Exchange Service Provider clarified reporting procedures and the framework of command and supervision covering outsourced contractors in preparation for IT system failures, etc.?

(iii) Upon occurrence of an IT system failure, etc. that may significantly affect its business operations, is the Crypto-Asset Exchange Service Provider prepared to promptly notify the representative director and other directors and report the greatest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect users, the reporting persons should not underestimate the risk but immediately report the highest risk scenario)?
In addition, is it prepared to launch a task force, have the representative director, etc. issue appropriate instructions and orders, and seek resolution of the issue in a swift manner?

(iv) Has the Crypto-Asset Exchange Service Provider clearly established the support framework for IT system failures, etc. to promptly gather experts having relevant know-how and experience from the IT Systems Department, other departments, or outsourced contractors, for example, through prior registration of these experts?

(v) When an IT system failure, etc. occurs, does the Crypto-Asset Exchange Service Provider disclose the details of the failure, the cause of the failure, and expected recovery time, and does it promptly take measures, such as establishing call centers and consultation desks as necessary, and asking the Association for help in responding, if it is a member of the Association, in order to properly respond to inquiries from customers?
Also, does the Crypto-Asset Exchange Service Provider clarify arrangements and procedures as to how to provide relevant business departments with necessary information in preparation for IT system failures, etc.?

(vi) Has the Crypto-Asset Exchange Service Provider conducted analysis of causes of IT system failures, etc., investigation about impact until recovery, corrective action, and preventive measures for recurrence based on its analysis of the underlying causes in a proper manner?
Also, does it prepare an IT system failure record ledger or any other similar document,

periodically analyze tendencies of factors that have led to such IT system failures, etc., and take measures according to them?

(vii) Has the Crypto-Asset Exchange Service Provider established a systematic framework to minimize impacts of IT system failures, etc., such as a system to bypass the affected part?

Reference: As reference materials relating to the IT system risk, there are, for example, "FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions" (The Center for Financial Industry Information Systems).

II-2-3-1-3 Responses in the Event of IT System Failures, etc.

The supervisors shall require a Crypto-Asset Exchange Service Provider, upon finding occurrence of an IT system failure or cybersecurity incident, to immediately notify the relevant authorities of the fact and then to make a report to the authorities in a form of the "Report on Occurrence of IT System Failure" (Appended Form 1). In addition, the Crypto-Asset Exchange Service Provider is also required to submit a report on recovery of the system and causes of the system failure when they are identified. Note that in cases where the failure causes are not identified, the Crypto-Asset Exchange Service Provider must report the actual situation within one month from the occurrence of the IT system failure.

Upon receipt of a report from the Crypto-Asset Exchange Service Provider, Local Finance Bureaus shall immediately contact the relevant division of the Financial Services Agency.

(i) IT system failures, etc. that must be reported

Failure or trouble that occurred in IT systems and devices (both hardware and software) currently used by a Crypto-Asset Exchange Service Provider for whatever reason, and

(A) that delays or suspends, or may delay or suspend business operations pertaining to the Crypto-Asset Exchange Services; or

(B) that may otherwise be deemed similar to above in the course of business.

However, even though some of the systems and equipment have such troubles, the reporting requirement is not applicable in cases where a backup system has quickly started up and effectively prevented adverse effects.

Even though a failure or trouble does not actually occur, a Crypto-Asset Exchange Service Provider is required to make a report when the users or business operations are affected or highly likely to be affected because it receives an advance notice of cyberattack or it has found a cyberattack in its IT systems.

(ii) The supervisory authorities shall require the Crypto-Asset Exchange Service Provider to submit an additional report pursuant to Article 63-15 of the Act, as needed, and if it is found that the Crypto-Asset Exchange Service Provider has a serious problem, the supervisory authorities shall issue an order to improve business operations pursuant to Article 63-16 of the Act.

(iii) In particular, when a major failure has occurred, or when it takes considerable time for the Crypto-Asset Exchange Service Provider to solve the causes of the failure, the supervisory authorities, while watching the Crypto-Asset Exchange Service Provider activate its contingency plan, including general announcement of the details of the failure to the public and responses to users at its website, etc., requires the Crypto-Asset Exchange Service Provider to promptly identify the causes, and requires a prompt report pursuant to Article 63-15 of the Act.

II-2-3-1-4 Responses at the Time of IT System Update and Integration, etc.

When an Crypto-Asset Exchange Service Provider updates or integrates important IT systems, the supervisors require the Crypto-Asset Exchange Service Provider to submit a report based on Article 63-15 of the Act as needed, and confirm plans and progress, as well as the appropriateness and effectiveness of project management, and then take actions such as issuing an order for business improvement based on Article 63-16 of the Act if significant problems are found.

II-2-3-2 Administrative Risk Management

II-2-3-2-1 Purpose and Significance

Administrative risk refers to the risk that a Crypto-Asset Exchange Service Provider incurs a loss due to its officers and/or employees failing to perform accurate administrative work or due to their problematic conducts or wrongful acts. Crypto-Asset Exchange Service Providers need to strive to ensure their reliability and creditworthiness by properly developing an internal control environment regarding administrative risk and maintaining the soundness and appropriateness of their business operations. The following points, for example, shall be taken into consideration.

II-2-3-2-2 Major Supervisory Viewpoints

(1) Control environment for managing administrative risk

(i) Has the Crypto-Asset Exchange Service Provider developed an appropriate control environment for managing administrative risk based on the understanding that such risk is involved in all business operations?

(ii) Has the Crypto-Asset Exchange Service Provider implemented specific measures to reduce administrative risk based on the recognition of the importance of reducing such risk? For example, conceivable measures to prevent problematic conducts and wrongful acts by the department in charge of administrative work include having an IT system serve a checking function, and establishing a checking procedure whereby several persons are in charge of checking.

(iii) Has the Crypto-Asset Exchange Service Provider developed a control environment wherein the department in charge of administrative work is able to perform the internal check-and-balance function sufficiently? Also, has the Crypto-Asset Exchange Service Provider established rules and regulations regarding administrative work and processes?

(iv) Does the Crypto-Asset Exchange Service Provider treat important legal compliance issues relating to verification at the time of transactions and submission of a notification of "suspicious transactions" as a legal compliance issue to deal with on a company-wide basis, rather than processing them as a mere administrative problem?

(v) In cases where the proper and secure conduct of business of the Crypto-Asset Exchange Service Provider is not ensured due to its officers and/or employees failing to perform accurate administrative work or due to their problematic conducts or wrongful acts, does the Crypto-Asset Exchange Service Provider make necessary notifications and take necessary measures as a misconduct based on II-2-1-6?

(2) Administrative risk management by internal audit function

Does the Internal Audit Department properly conduct internal audits in order to examine the control environment for managing administrative risk?

(3) Control environment for managing administrative risk in business offices

Has the division in charge of managing administrative risk at headquarters taken measures for checking business offices' control environments for managing administrative risk?

II-2-3-3 Outsourcing

II-2-3-3-1 Purpose and Significance

Even when a Crypto-Asset Exchange Service Provider outsources part of its business to a third party (including multi-tiered outsourcing), the Provider is not exempted from the final responsibility pertaining to such outsourced work. Therefore, in order to ensure the protection of users and the proper and secure conduct of the business, it is necessary to pay attention to the following points, for example, depending on the nature of the business of the Crypto-Asset Exchange Service Provider. It should be noted that the following points are only general points of view, and additional verification may be required, depending on the content of the outsourced work.

Note: In supervising matters related to outsourcing, the supervisors shall basically grasp the facts of a case, etc. through an interview from the Crypto-Asset Exchange Service Provider, who is the outsourcer. However, in light of the urgency and seriousness of the case, the supervisors shall consider having an interview with outsourced contractors in parallel as needed.

When having an interview with an outsourced contractor, the supervisors shall ask the Crypto-Asset Exchange Service Provider, who has outsourced its service to the outsourced contractor, to attend the interview as needed.

II-2-3-3-2 Major Supervisory Viewpoints

(i) Has the Crypto-Asset Exchange Service Provider established internal rules, etc. stipulating criteria for selecting contractors or measures to be taken when outsourcing risk appears, and disseminated them company-wide such internal rules, etc. through internal training, etc. so that its officers and employees properly handle cases in accordance with such internal rules, etc.?

(ii) Does the Crypto-Asset Exchange Service Provider select outsourced contractors from the viewpoints of whether they can provide services at a sufficient level in light of its business details and scale, and whether they can provide services in accordance with contracts and perform other contractual obligations?

(iii) Has the Crypto-Asset Exchange Service Provider taken appropriate measures regarding the development of a legal compliance system at the outsourced contractor, such as issuing necessary instructions? In addition, has the Crypto-Asset Exchange Service Provider taken measures to ensure that outsourcing does not hinder the performance of obligations to supervisory authorities regarding inspections, reporting orders, submission of records, etc.?

(iv) Has the Crypto-Asset Exchange Service Provider made it clear that the outsourcing of business operations does not cause any change in the contractual rights and obligations involving it and its users and that the users continue to have the same rights as if the business operations were conducted by the Crypto-Asset Exchange Service Provider itself?

Note: Outsourcing includes cases where a Crypto-Asset Exchange Service Provider is deemed to substantially outsource its business to an external contractor even if a formal contract is not concluded or where the outsourced work is performed overseas.

(v) Has the Crypto-Asset Exchange Service Provider developed a control environment that prevents users from suffering inconveniences if the Crypto-Asset Exchange Service Provider

cannot be provided with the services agreed under the outsourcing contract with its outsourced contractor?

(vi) When outsourcing the handling of information of individual users to an outsourced contractor, has the Crypto-Asset Exchange Service Provider taken the measures to supervise the outsourced contractor as necessary and appropriate measures to prevent such information from being leaked, lost, or damaged based on Article 10 of the Financial Sector Personal Information Protection Guidelines and III of the Practice Guidelines?

(vii) With regard to the management of outsourced contractors, does the Crypto-Asset Exchange Service Provider clarify the responsible division and confirm that outsourced contractors are properly managing information related to users, such as by monitoring on a periodic or as-needed basis how business operations are being conducted at outsourced contractors?

(viii) Has the Crypto-Asset Exchange Service Provider confirmed that outsourced contractors have systems in place to take appropriate actions and to promptly report to the Crypto-Asset Exchange Service Provider in the event that information is leaked, lost, or damaged at outsourced contractors?

(ix) Does the Crypto-Asset Exchange Service Provider restrict the access right by outsourced contractors to the information related to users possessed by the Crypto-Asset Exchange Service Provider to the extent necessary according to the nature of the outsourced business?
On that basis, does the Crypto-Asset Exchange Service Provider check whether the officers and employees at outsourced contractors to whom access rights are given have been defined, along with the scope of their access rights?
Furthermore, does the Crypto-Asset Exchange Service Provider confirm that the access rights are being managed thoroughly at outsourced contractors on a periodic or as-needed basis, such as by checking how the access rights are used (including crosschecking authorized persons with actual users) in order to prevent the access rights assigned to certain people from being used by others?

(x) In cases of multi-tiered outsourcing, does the Crypto-Asset Exchange Service Provider check whether the outsourced contractor is adequately supervising its subcontractors and other business operators? In addition, does the Crypto-Asset Exchange Service Provider directly supervise such subcontractors and other business operators as needed?

(xi) With regard to complaints, etc. pertaining to the outsourced service, has the Crypto-Asset Exchange Service Provider developed an appropriate complaint consultation system, such as a system to accept direct communication from users to the Crypto-Asset Exchange Service Provider who outsourced such service?

II-2-4 Responses to Persons with Disabilities

II-2-4-1 Purpose and Significance

The Act for Eliminating Discrimination against Persons with Disabilities (Act No. 65 of 2013; hereinafter referred to as the "Disability Discrimination Act") prohibits a company from engaging in unfair discriminatory treatment for persons with disabilities and requires it to make efforts to improve reasonable accommodation to implement elimination of social barriers.

In addition, the "Guidelines concerning Promotion of Elimination of Discrimination on the Basis of Disability in Business Fields under the FSA's Jurisdiction" (Public Notice No. 3 of 2016; hereinafter referred to as the "Guidelines for Eliminating Discrimination against Persons with Disabilities") specify how Crypto-Asset Exchange Service Providers should respond to those with disabilities.

When supervising the response to persons with disabilities, the following points shall be taken into

consideration in light of the abovementioned intent.

II-2-4-2 Major Supervisory Viewpoints

Has the Crypto-Asset Exchange Service Provider developed an internal control environment for responding to persons with disabilities, such as by taking appropriate actions in accordance with the Disability Discrimination Act and the Guidelines for Eliminating Discrimination against Persons with Disabilities including in terms of user protection and user convenience, and by grasping and verifying the response status and reviewing response methods?

II-3 Supervisory Methods and Measures

With regard to issues and challenges, etc. concerning the business management or the appropriateness of the business of the Crypto-Asset Exchange Service Provider, which have been identified through the follow-up to the matters indicated in the inspection and the daily supervisory administration such as the notification of misconduct, etc., the supervisory authorities shall monitor the status of voluntary business improvement made by such Crypto-Asset Exchange Service Provider, by holding an in-depth interview regarding the cause of the issue, improvement measures, etc. and, when necessary, collecting a report based on Article 63-15 of the Act, based on the viewpoints mentioned above.

Furthermore, if it is found that the Crypto-Asset Exchange Service Provider has a serious problem from the viewpoint of protecting the interests of its users, the supervisory authorities shall issue an order to improve business operations pursuant to Article 63-16 of the Act. If a serious and/or malicious violation of laws and regulations is found, the supervisory authorities shall consider issuing an order to suspend business, etc. based on Article 63-17 of the Act (See III-3 for matters to be taken into consideration when conducting administrative dispositions).

II-4 Points to Note Regarding Supervision of Non-member Providers

II-4-1 Purpose and Significance

Article 63-17(1)(i) of the Act stipulates that, if a Crypto-Asset Exchange Service Provider that does not join the Association (hereinafter referred to as a "Non-member Provider" in II-4) is deemed as "a corporation that has not prepared internal rules that have contents equivalent to the articles of incorporation or other rules of the Certified Association for Payment Service Providers or has not established a system for ensuring compliance with those internal rules" prescribed in Article 63-5(1)(vi) of the Act, the Crypto-Asset Exchange Service Provider shall be subject to the rescission of registration, etc. In light of these provisions, when supervising Non-member Providers, the supervisors shall pay attention to the following points.

II-4-2 Major Supervisory Viewpoints

(i) Has the Non-member Provider properly prepared internal rules that have contents equivalent to the Articles of Incorporation or other rules of the Association (hereinafter referred to as "Association Rules"?

(ii) Has the Non-member Provider established frameworks to ensure appropriate compliance with internal rules (such as making them known to all officers and employees, giving training to employees, and verifying the compliance status, etc.)

(iii) When Association Rules are revised, does the Non-member Provider make it sure to review its internal rules immediately in accordance with the revision?

II-4-3 Supervisory Methods and Measures for Non-member Providers

In cases where a problem is found with regard to the formulation, revision, or compliance status, etc. of the internal rules of a Non-member Provider, the supervisors shall monitor the status of voluntary business improvement made by the Crypto-Asset Exchange Service Provider by holding an in-depth interview and, when necessary, requiring a report based on Article 63-15(1)of the Act, Also, if it is found that the Crypto-Asset Exchange Service Provider has a serious problem from the viewpoint of protecting the public interest or user protection, the supervisory authorities shall take actions such as issuing an order to improve business operations based on Article 63-16 of the Act. Furthermore, if the submitted report indicates that the Crypto-Asset Exchange Service Provider is not deemed to have prepared internal rules that have contents equivalent to the Association Rules or that it has not established a system to comply with such internal rules, the supervisory authorities shall consider necessary actions, including the issuance of an order to suspend business based on Article 63-17 of the Act.

II-5 Basic Views on Foreign Crypto-Asset Exchange Service Providers

II-5-1 Prohibition of Solicitation by Foreign Crypto-Asset Exchange Service Providers

Foreign Crypto-Asset Exchange Service Providers (excluding those registered under the Act; the same shall apply hereinafter in II-5-2) must not solicit any person in Japan for transactions pertaining to the Crypto-Asset Exchange Services, unless otherwise provided for by laws and regulations.

Note: It should be noted that when a business operator located overseas, including a foreign Crypto-Asset Exchange Service Provider, is engaged in Exchange of Crypto-Assets, etc. with a person located in Japan in the course of trade, the act of the business operator falls under the category of the Crypto-Asset Exchange Services.

II-5-2 Cross-Border Transactions by Foreign Crypto-Asset Exchange Service Providers Using the Internet, etc.

An act of posting an advertisement, etc. concerning transactions pertaining to the Crypto-Asset Exchange Services on a website, etc. by a foreign Crypto-Asset Exchange Service Provider generally falls under the act of "soliciting/solicitation."

Provided, however, that the foregoing shall not apply to "soliciting/solicitation" directed to a person in Japan as long as reasonable measures, including the measures set forth below, are taken so as not to result in any transactions pertaining to the Crypto-Asset Exchange Services with a person in Japan.

(1) Disclaimer

Clearly state that persons in Japan are not covered by the service.

The following points should be taken into consideration when determining whether the above measures have been taken sufficiently.

(i) No particular operation of computer or device other than viewing the advertisement is required for reading and understanding the disclaimer.

(ii) The disclaimer must be indicated in language reasonably deemed to be readable and understandable for those in Japan who are accessing the website.

(2) Measures to prevent transactions

Measures must be taken to prevent transactions pertaining to the Crypto-Asset Exchange Services with a person in Japan.

The following points should be taken into consideration when determining whether the above

measures have been taken sufficiently.

(i) At the time of a transaction, the business operator has gone through the procedure to confirm the residence of the user by having the user present his/her address, mailing address, e-mail address, payment method, and other information.

(ii) In cases where there are reasonable grounds to believe that it is clearly a transaction pertaining to the Crypto-Asset Exchange Services by a person in Japan, the business operator should take care not to accept the order from the person in Japan.

(iii) The business operator has been attentive in order not to conduct any act of inducing persons in Japan to engage in transactions pertaining to the Crypto-Asset Exchange Services, including establishing a call center for users in Japan or linking websites targeted at persons in Japan.

In addition, the measures listed above are merely examples, and if equivalent or superior measures are taken, posting of advertisements, etc. shall not be deemed to be an act of "soliciting/solicitation" for persons in Japan.

(3) In cases where reasonable measures described above are not taken, since the posting of advertisement, etc. is highly likely to be deemed as the act of "soliciting/solicitation" of transactions pertaining to the Crypto-Asset Exchange Services for persons in Japan, the foreign Crypto-Asset Exchange Service Provider should prove that it has not conducted any transactions pertaining to the Crypto-Asset Exchange Services with persons in Japan, including any solicitation thereof. III Points to Note regarding Administrative Processes to Note Regarding Supervision of Crypto-Asset Exchange Service Providers.

III. Points to Note regarding Administrative Processes to Note Regarding Supervision of Crypto-Asset Exchange Service Providers

III-1 General Administrative Processes, etc.

III-1-1 Basic Views on Inspection and Supervision

The purpose of inspecting and supervising a Crypto-Asset Exchange Service Provider is to enforce registration and provide other necessary measures with respect to Exchange of Crypto-Assets, etc. in order to ensure the appropriate provision of payment services, and protection of the users, etc. thereof, and to promote the provision of those services, thereby contributing to the improvement of the safety, efficiency, and convenience of the payment and settlement system (see Article 1 of the Act).

To accomplish the purpose of such inspection and supervision, the supervisory authorities need to make continuous responses commensurate with the scale and characteristics of each Crypto-Asset Exchange Service Provider.

For this, in conducting the inspection and supervisory affairs of Crypto-Asset Exchange Service Providers, it is essential to first understand the policies of how each Crypto-Asset Exchange Service Provider intends to address issues and challenges in developing business models and establishing compliance management and risk management systems, and then to accurately understand how these policies are implemented, what governance systems are operated for such implementation, what potential risks or problems lurk, and how Crypto-Asset Exchange Service Providers recognize and respond to their respective risks and problems.

Based on this approach, each Crypto-Asset Exchange Service Provider itself needs to transform its management structure so that it can work on continuous improvement toward the best practices on its own without being pointed out by the supervisory authorities. The supervisory authorities will

encourage each Crypto-Asset Exchange Service Provider to pursue its efforts in seeking better practices through continuous monitoring through fact-finding and dialogue.
However, if, in the course of such monitoring activities, the supervisors find any issue that is considered serious in terms of the soundness and appropriateness of the Crypto-Asset Exchange Service Provider's business or find that the Crypto-Asset Exchange Service Provider is unable to improve its business by its self-initiated efforts only, the supervisors shall consider whether to issue an order to improve business operations pursuant to Article 63-16 of the Act or to impose other administrative disposition (as explained in III-3).
Some other points that need to be adequately considered in the course of supervising Crypto-Asset Exchange Service Providers are summarized as follows.

(1) Ensuring sufficient communication with Crypto-Asset Exchange Service Providers
In inspecting and supervising a Crypto-Asset Exchange Service Provider, it is important to adequately gather and analyze information about the business operations of the Crypto-Asset Exchange Service Provider and to respond appropriately and in a timely manner. For this reason, the supervisory authorities should, in addition to obtaining reports from Crypto-Asset Exchange Service Providers, endeavor to closely communicate with them and collect information on a day-to-day basis under sound and constructive tension with Crypto-Asset Exchange Service Providers. More specifically, it is necessary to ensure daily communication with Crypto-Asset Exchange Service Providers through regular and timely interviews and exchanges of opinions with various officers and employees thereof, including the management team, outside directors, and persons in charge of internal audits, and to endeavor to grasp not only financial information but also various information on management.

(2) Respect for voluntary efforts of Crypto-Asset Exchange Service Providers
While each of Crypto-Asset Exchange Service Providers, as a private company, makes management decisions at its own risk and responsibility, the role of the supervisory authorities is to review such decisions based on relevant laws and regulations and to encourage each of them to resolve problems by its own efforts and resources. With this role firmly in mind, the supervisors must pay due regard to the initiatives of Crypto-Asset Exchange Service Providers in their business operations throughout supervisory processes.

(3) Ensuring efficient and effective inspection and supervisory
From the viewpoint of making effective use of limited resources of the supervisory authorities and Crypto-Asset Exchange Service Providers, it is necessary to conduct inspection and supervisory activities efficiently and effectively while taking into consideration the scale and characteristics of Crypto-Asset Exchange Service Providers. Therefore, when the supervisors ask a Crypto-Asset Exchange Service Provider to submit reports or other documents, the scope of such documents must be limited to the extent truly necessary for the relevant supervisory processes. More importantly, the supervisors must continue efforts to enhance efficiency and effectiveness of supervisory activities; the necessity of the supervisory processes currently adopted and their methodologies should be constantly reviewed and supervisory processes should be redesigned whenever necessary.
The content of the reports previously obtained from Crypto-Asset Exchange Service Providers and the procedures for requesting submission of reports or documents are reviewed once every year to streamline such procedures and reduce paperwork burdens of Crypto-Asset Exchange

Service Providers. On such occasions, the supervisors should seek opinions of Crypto-Asset Exchange Service Providers about submission requirements.

(4) In cases where a Crypto-Asset Exchange Service Provider belongs to a financial-related group (Note 1) that includes multiple financial institutions, the supervisors should strive to perform supervisory processes in accordance with the actual situation of the financial-related group. It is important to examine the effectiveness of business management (Note 2), the appropriateness of capital adequacy (Note 3), the appropriateness of identifying and managing risks (Note 4), and its compliance frameworks (Note 5) as a financial-related group, and to take necessary measures.

Note 1: A group of financial institutions of various business types under the control of a parent-child relationship or holding company, etc. (This group includes subsidiaries and affiliates of these companies as well as companies that provide internal control services for these companies.)

Note 2: For example, the effectiveness of "representative directors, directors, and the Board of Directors", "company auditors and the Board of Company Auditors", and the "Internal Audit Department"

Note 3: For example, the appropriateness of capital adequacy of both the Crypto-Asset Exchange Service Provider within the financial-related group and the financial-related group itself

Note 4: For example, the spread, uneven distribution, or concentration of risks, and the appropriateness of the control environment for various risks

Note 5: For example, compliance frameworks, appropriateness of transactions within the financial-related group, control environment for administrative risk/IT system risk, control environment for managing a crisis, capital increase, protection of customer information, and development of systems to protect customers' interests

(5) Ensuring cooperation with overseas supervisory authorities, etc.

With respect to the FSA's response to overseas activities of a Crypto-Asset Exchange Service Provider or the like and those of an unregistered business operator or the like (which refers to the "unregistered business operator or the like" as defined in III-1-6(1)), the FSA needs to closely coordinate with the financial supervisory authorities in the countries (the host countries) in which the Crypto-Asset Exchange Service Provider or the like and the unregistered business operator or the like have operation bases, respectively.

(6) Active information gathering about Crypto-Asset Exchange Service Providers

In the inspection and supervision of Crypto-Asset Exchange Service Providers, it is important for the supervisors to accurately understand and analyze information on the management of Crypto-Asset Exchange Service Providers, including complaints, etc. from users, etc., and to take appropriate and timely measures for inspection and supervision as necessary. For this reason, it is necessary to pay attention not only to reports from Crypto-Asset Exchange Service Providers but also to complaints from users, etc., and to actively collect information through daily and sufficient communication with the Association and Crypto-Asset Exchange Service Providers.

III-1-2 How to Supervise Crypto-Asset Exchange Service Providers

The supervision over Crypto-Asset Exchange Service Providers is basically intended to encourage their necessary improvements. Such supervisory activities are implemented by combining various approaches and methods, including monitoring through fact-finding and dialogue, imposition of

administrative measures, giving feedback, and dissemination of information. Such approaches and methods should be appropriately chosen based on individual Crypto-Asset Exchange Service Providers' circumstances and the characteristics and severity of their problems.
In addition, through day-to-day monitoring, the supervisors are required to accurately grasp changes in the global economy and market environments that could affect Crypto-Asset Exchange Service Providers from the viewpoint of ensuring the appropriate provision of payment services and protecting users. Also, with regard to individual Crypto-Asset Exchange Service Providers' circumstances, the supervisors are required to encourage their efforts to pursue best practices for risk management practices, etc., to develop management and governance systems capable of flexibly responding to changes, and to resolve various challenges through dialogue with Crypto-Asset Exchange Service Providers, based on data obtained from monitoring and findings from occasional interviews.

III-1-3 Supervisory Approaches and Methods

(1) Continuous and seamless monitoring focused on priority issues

The supervisory authorities shall identify the characteristics and issues of each Crypto-Asset Exchange Service Provider, and depending on the nature and priority of those issues, chooses among and flexibly uses various monitoring methods (including on-site inspection). Continuous monitoring is required by following up on the progress of Crypto-Asset Exchange Service Providers' improvement activities.

With regard to the selection of monitoring methods, in addition to the specific and situation of each Crypto-Asset Exchange Service Provider, the effectiveness of each monitoring method in the given situation, workload burdens of both the supervisory authorities and the Crypto-Asset Exchange Service Provider, and the urgency of the issues, etc. should be fully considered. In general, what comes first is to conduct monitoring through analyses of the Crypto-Asset Exchange Service Provider's business performance, financial performance, and other information or through interviews with the Crypto-Asset Exchange Service Provider's personnel and its stakeholders within and outside the Crypto-Asset Exchange Service Provider. On this occasion, whether or not the Crypto-Asset Exchange Service Provider's business is sound and appropriate for the time being is analyzed. Based on the analysis findings, whether or not to conduct on-site inspection under Article 63-15 of the Act will be determined.

The specific implementation of monitoring shall be based on III-1-2. In addition, such monitoring shall be based on the "Questionnaire on Registration Screening of Crypto-Asset Exchange Service Providers," which supplements and extends the supervisory viewpoints in these Guidelines and is a tool to facilitate dialogue with these business operators, and the contents of the self-regulatory rules set by the Association.

(2) Methods for supervisory activities

(i) Actions necessary for understanding the Crypto-Asset Exchange Service Provider's circumstances and conducting dialogues

(A) Information gathering and profiling (recognition of characteristics)

As mentioned above, the FSA conducts monitoring with the intention of grasping specific circumstances of each Crypto-Asset Exchange Service Provider from time to time, such as its characteristics, challenges, and the status of self-initiated efforts for improvement. Such monitoring activities include the step of understanding impacts of changing business environments on the Crypto-Asset Exchange Service Provider's business management and

its response.

These information gathering and profiling activities are accumulated through day-to-day monitoring. While no particular forms or methods are designated for these activities, the perspectives illustrated below may be informative.

a) Macro-level perspectives

It is necessary to identify and analyze impacts of changes in domestic or international environments such as economy, financial markets, politics, and societies on individual Crypto-Asset Exchange Service Providers. One useful way is, for example, to seek cooperation from relevant bureaus and divisions in the FSA, Local Financial Bureaus, or other relevant ministries or governmental agencies to gather various information about changes in domestic and international environments. Such information may cover cases of misconduct committed by domestic and international companies, including enterprises in non-financial sectors; legislative changes, system reforms, and trends of judicial precedents in Japan and overseas; developments in discussions by foreign regulators or international organizations; Crypto-Asset trading market trends; economic or social changes; and progress in technology used in Crypto Assets. Analyses of such various information may reveal common challenges which are faced by industry peers or firms in other industries, which can be observed in similar products or services, or which may exist in legislative systems.

Through such information gathering and analysis activities described above, the supervisory authorities shall analyze the horizontal development and spread of problems observed and strive to identify and highlight problems inherent in Japan's Crypto-Asset Exchange Service Providers as a whole.

b) Micro-level perspectives

For effective dialogue and other communication with Crypto-Asset Exchange Service Providers, it is essential to accumulate extensive knowledge about the specific conditions of individual Crypto-Asset Exchange Service Providers. Among other measures, the first thing to do is to check each Crypto-Asset Exchange Service Provider's management philosophy, such as what the Crypto-Asset Exchange Service Provider aims to be in its business environment (e.g., customer characteristics, competitive environment) and what the Crypto-Asset Exchange Service Provider wants to do toward this end, as well as its business model, management strategy, business operations, and organizational frameworks based on the management philosophy. It is advisable to gather the information illustrated below from each Crypto-Asset Exchange Service Provider and its stakeholders (e.g., employees, customers, shareholders).

- The scope of information to be analyzed should not be limited to typical information such as business and financial conditions, but should be extended to minutes of executive meetings or other organs and documents pertaining to management decisions (including the information about the identification and evaluation of management risks).
- In addition to interviews in connection with the Crypto-Asset Exchange Service Provider's financial results or risk management, interviews should be held from time to time with the heads of the Crypto-Asset Exchange Service Provider's respective business units and other officers or managers in different positions in order to learn about the Crypto-Asset Exchange Service Provider's business conditions, the status of ensuring proper business operations, or other activities.

- To understand how the Crypto-Asset Exchange Service Provider perceives its risks and what its business operations ought to be, the supervisors need to exchange views with the Crypto-Asset Exchange Service Provider's Internal Audit Department, Audit Committee members, company auditors, outside directors, etc.
- Feedback from users of financial services can be obtained through various channels, and such feedback includes, for example, inquiries or complaints, etc. received at FSA's Counseling Office for Financial Services Users. In addition, media reports, inquiries from third parties, and other external information should be analyzed.

(B) Identification of priority issues and formulation of monitoring policies and plans

After horizontal challenges common among individual Crypto-Asset Exchange Service Providers and business categories are identified through the information gathering and profiling activities described above, all those issues shall be prioritized, taking into full consideration the degree of importance and urgency of the occasion such as social demands. This prioritization is necessary to facilitate subsequent discussions between the supervisory authorities and each Crypto-Asset Exchange Service Provider's executives on substantive issues critical to its business and to make maximum use of limited administrative resources. The horizontal challenges identified as priority issues in this process are published in the supervisory authorities' annual supervisory policies at the beginning of each fiscal year.

Subsequently, it is necessary to formulate monitoring policies and plans based on each Crypto-Asset Exchange Service Provider's specific conditions, to determine practical policies and plans to address priority issues, and to establish a system for appropriate staffing, etc. To enable Crypto-Asset Exchange Service Providers to concentrate their management resources on efforts to address critical and substantive problems, the supervisory authorities shall choose between on-site inspection and other monitoring methods, and between each Crypto-Asset Exchange Service Provider-specific monitoring and horizontal monitoring, depending on the nature of priority issues.

Rather than being conducted periodically, on-site inspections are considered to be one of the methods incorporated in continuous and seamless monitoring processes to grasp the actual condition of individual Crypto-Asset Exchange Service Providers. However, if on-site inspections have not been conducted for a long period of time, it is considered to be one of the risk factors that the possibility of problematic events occurring which are unforeseeable by supervisory authorities is relatively high.

In the event that new issues arise or are uncovered during the fiscal year, the supervisory authorities shall flexibly adjust monitoring plans and endeavor to adapt monitoring activities for changing circumstances.

(ii) Detailed understanding of each Crypto-Asset Exchange Service Provider's circumstances

To figure out individual Crypto-Asset Exchange Service Providers' actual conditions, the supervisory authorities shall chose the most efficient and effective methods among: various interviews, requesting submission of documents on a non-compulsory basis, questionnaires, demanding submission of statutory reports, on-site inspection, and other methods. Which to choose depends on the nature of issues to be addressed, the progress of countermeasures being implemented, and other circumstances specific to each Crypto-Asset Exchange Service Provider.

If the supervisory authorities have received reports from Crypto-Asset Exchange Service Providers through any previous monitoring or have already obtained some information about

Crypto-Asset Exchange Service Providers from other sources, the supervisors must review them in advance and effectively use the information on hand in order to mitigate the Crypto-Asset Exchange Service Providers' burdens.

If new or previously unpredicted issues come to the attention of the supervisors in the course of gathering information, understanding of actual conditions, or dialogue after the monitoring based on the previous analyses, the supervisors shall make appropriate responses in light of the nature of the new issues.

When applying any monitoring method, the points illustrated below should be considered. Regardless of which method is chosen, the supervisory authorities must clearly explain the problems recognized by the supervisory authorities and the purpose of discussions with the Crypto-Asset Exchange Service Provider.

(A) Interviews

In order to deepen mutual understanding with Crypto-Asset Exchange Service Provider on its priority issues, the supervisory authorities shall conduct multilevel interviews with the Crypto-Asset Exchange Service Provider's personnel, including top executives, the heads of business departments, and working-level managers, depending on the nature of the issues.

The pursuit of best business practices is a matter that each Crypto-Asset Exchange Service Provider should voluntarily promote to find its own way appropriate for its own conditions and circumstances. With this view in mind, the supervisory authorities should not impose a particular solution on the Crypto-Asset Exchange Service Provider.

As part of these interviews, the supervisory authorities may conduct interviews or discussions on specific themes on Crypto-Asset Exchange Service Providers' premises intensively for a certain period of time.

(B) Requesting submission of documents on a non-compulsory basis

When requesting Crypto-Asset Exchange Service Providers to submit documents, the supervisory authorities shall pay due regard to their burdens and closely communicate with the Crypto-Asset Exchange Service Providers in advance, in order to convince the Crypto-Asset Exchange Service Providers of what documents are desired and why they are necessary, through clear and accurate explanations. The supervisors should try to reduce Crypto-Asset Exchange Service Providers' burdens by asking for submission at multiple times with adequate intervals, avoiding duplicated submission requests, and allowing sufficient time before submission deadlines. When asking multiple Crypto-Asset Exchange Service Providers for submission of documents at the same time (e.g., questionnaires), due regard should be given to respective Crypto-Asset Exchange Service Providers' characteristics and circumstances.

(C) Request for reporting under Article 63-15 of the Act

When it is found necessary, the supervisory authorities shall ask a Crypto-Asset Exchange Service Provider to make a report pursuant to Article 63-15 of the Act. In this event, the Crypto-Asset Exchange Service Provider must be fully informed and convinced as to why such reporting is requested and how the supervisory authorities perceive the Crypto-Asset Exchange Service Provider's issues.

(D) On-site inspection pursuant to Article 63-15 of the Act

The supervisors shall conduct on-site inspection pursuant to Article 63-15 of the Act when the supervisors determine that detailed examination is required to verify the soundness and appropriateness of the current business of a Crypto-Asset Exchange Service Provider, or

when it is found necessary on other grounds. In doing so, the supervisors shall always keep in mind what are the most important management issues and what are the underlying causes of these issues, and reaffirm the accuracy of the selection and definition of priority issues together with the Crypto-Asset Exchange Service Provider's executives, and to form hypotheses. To demonstrate the hypotheses, the supervisors shall gather and analyze more detailed information about the facts and circumstances and continue discussions with the Crypto-Asset Exchange Service Provider's executives based on additional analyses. Such discussions should not end up in seeking a facile solution, but should aim at a fundamental solution of the problems critical in terms of both the Crypto-Asset Exchange Service Provider's management and the financial administration.

In this regard, see the Basic Procedures for On-Site Inspection, as shown in Exhibit 1. If the supervisors issues a notice of inspection results to an inspected Crypto-Asset Exchange Service Provider, the supervisors shall, within one week after the notice in principle, ask the Crypto-Asset Exchange Service Provider to report its fact-checking of the problems pointed out in the notice, its own analyses of the causes of those problems, planned measures for improvement or remediation, and other comments within one month pursuant to Article 63-16 of the Act. With regard to the matters required to be reported, adequate and sufficient reportable matters should be specified on an individual basis in a way tailored to the problems detected in the inspection.

(iii) Dialogue

Dialogue with a Crypto-Asset Exchange Service Provider shall be conducted to clarify whether any problem that could affect the Crypto-Asset Exchange Service Provider's management foundation or compliance has occurred or is likely to occur, to review the Crypto-Asset Exchange Service Provider's initiatives for enhancing business management, or to discuss other issues that are important under the present circumstances or in light of the nature of ongoing problems.

When holding a dialogue, the supervisors shall avoid imposing their beliefs or hypotheses and endeavor to make Crypto-Asset Exchange Service Providers feel free to express their views. After hearing their story and grasping their mindset and policies, the supervisors carry out fact-based discussions.

Furthermore, on each occasion of such dialogue session, the supervisors shall make efforts to ensure the continuity of the dialogue, taking into full consideration the communications made so far between the supervisory authorities and each Crypto-Asset Exchange Service Provider.

(A) If the supervisors determine, based on the facts ascertained, that the Crypto-Asset Exchange Service Provider is highly likely to face a serious problem on the management foundation or compliance, etc., the Crypto-Asset Exchange Service Provider will verify its issues, the root causes, and the adequacy of remediation measures first of all. Then, in-depth discussions between the supervisors and the Crypto-Asset Exchange Service Provider to implement remediation measures shall follow. If, however, a serious problem has already arisen or high urgency in any other form is observed, the supervisors may go further and pinpoint the issues which the supervisors consider necessary to be rectified and then check the policies of each Crypto-Asset Exchange Service Provider for rectification.

(B) If a Crypto-Asset Exchange Service Provider is determined to be unlikely to cause above-mentioned serious problems, the Provider is expected to exercise diverse initiatives to innovate itself in ways fitting its circumstances and to continue efforts to refine business models and risk management practices. The supervisory authorities shall try to deepen the

understanding of the business conditions and challenges of Crypto-Asset Exchange Service Providers and their policies and strategies through day-to-day monitoring and profiling activities. Then, the supervisory authorities shall conduct in-depth dialogue with Crypto-Asset Exchange Service Providers to discuss their business models, risk management practices, human resources development, and other issues, without a presumption on specific answers, for the purpose of promoting their improved awareness and understanding (and share model cases of other Crypto-Asset Exchange Service Providers for best practices where appropriate).

(iv) Flexible and appropriate use of various methods in combination

As explained before, the supervisory authorities may use various methods to make administrative responses to Crypto-Asset Exchange Service Providers. However, each method has some advantages and disadvantages in terms of effectiveness, workload burdens and expenses on the supervisory authorities and Crypto-Asset Exchange Service Providers. The supervisory authorities shall therefore flexibly choose among such methods, maximize their advantages, and seek their optimized combinations, aiming at even more effective and efficient supervisory activities. Which to choose and combine will depend on individual Crypto-Asset Exchange Service Providers' issues, the existence or non-existence of serious problems affecting their management foundation or compliance, or other individually specific ongoing circumstances. For example, the following methods may be available, in addition to the methods already explained.

- Feedback about industry-wide situations and challenges or theme-specific case examples will help encourage Crypto-Asset Exchange Service Providers' initiatives for innovation. In particular, feedback pertinent to a Crypto-Asset Exchange Service Provider's issues will help the supervisory authorities and the Crypto-Asset Exchange Service Provider build a shared vision and facilitate their in-depth dialogue. Even when giving such feedback, the supervisors shall respect individual Crypto-Asset Exchange Service Providers' business decisions and avoid unduly interfering with their judgments concerning specific transactions.
- The information voluntarily disclosed by Crypto-Asset Exchange Service Providers may cover their management policies and management reforms. Such information may not only facilitate dialogue between the Crypto-Asset Exchange Service Provider and the supervisory authorities, but also promote communication between the Crypto-Asset Exchange Service Provider and its customers or other stakeholders, which will back up the Crypto-Asset Exchange Service Provider's efforts for management reforms.
- If a Crypto-Asset Exchange Service Provider's problems pertain to user protection or convenience for customers, the supervisors shall contact the Crypto-Asset Exchange Service Provider's business partners, users, or other third parties for questionnaire surveys or interviews, rather than focusing on communication with the Crypto-Asset Exchange Service Provider only. Feedback from communication with such third parties will surely contribute to more effective dialogue between the supervisory authorities and the Crypto-Asset Exchange Service Provider.
- If the FSA can build a shared vision or goal with the stakeholders other than the Crypto-Asset Exchange Service Provider, as necessary, or if the FSA publicly discloses the findings from its analyses or the FSA's philosophy in financial administration, such activities may be helpful for convincing or appealing to stakeholders who are associated with Crypto-Asset Exchange Service Providers' business environments.

(v) Responses based on monitoring findings

The findings from the financial monitoring activities described above may be made known to the inspected Crypto-Asset Exchange Service Provider in any form without being caught up in the previous form of "notice of inspection results." Examiners may choose to confirm where the two sides disagreed and continue discussions. The supervisory authorities shall explore the best ways suitable for productive discussions focused on priority issues.

Feedback may be given to a Crypto-Asset Exchange Service Provider, for example, in any of the following ways when the supervisors intends to continue dialogue with the Crypto-Asset Exchange Service Provider, to ask for remedial necessary measures, or to carry out other adequate follow-up activities.

(A) If the supervisors conduct on-site inspection and off-site monitoring for a Crypto-Asset Exchange Service Provider over a full business year, the supervisors may compile the monitoring findings, as necessary, in the form of an annual monitoring report called a "Feedback Letter" and issue it to the Crypto-Asset Exchange Service Provider.

(B) Findings from on-site inspection shall be made known to the Crypto-Asset Exchange Service Provider, in principle, in each instance. Forms of providing feedback may vary depending on the types or severity of problems detected or the content of the on-site inspection. For example, when pointing out inconsequential problems or communicating with a Crypto-Asset Exchange Service Provider with low likelihood of causing serious problems as described in the above (iii)(B), the form of "Feedback," "Comments of supervisory authorities," or the like may be used. Meanwhile, the form of "Notice of Inspection Results" or the like will be used when warning about serious issues.

(C) In addition to the forms of communication described in (A) and (B) above, the supervisory authorities shall distribute information about industry-wide challenges to Crypto-Asset Exchange Service Providers from time to time.

Issues recognized and information gathered through monitoring activities shall be classified into the four categories as follows: (i) those applicable only to individual Crypto-Asset Exchange Service Providers, (ii) those applicable to the relevant business category, (iii) those applicable to other business categories, and (iv) those affecting other supervisory authorities' functions, related ministries and/or governmental agencies, or industry associations, etc. The issues classified above shall be incorporated in annual supervisory policies and monitoring plans for the subsequent fiscal year. In addition, consideration will be given to horizontal monitoring across business categories, and when a certain issue is likely to spill over into areas beyond the scope of the monitoring activities, the supervisory authorities shall seek cooperation from other supervisory authorities' functions, related ministries and/or governmental agencies, or industry associations, etc.

III-1-4 Quality Control

In order to ensure that proper judgments are made throughout all processes of inspection and supervision on the quality and depth of monitoring activities conducted through profiling and dialogue, the supervisory authorities perform organization-wide quality control. The supervisory authorities shall endeavor to secure the quality of its inspection and supervision activities so that financial functions can be maximized, based on broad perspectives of maximizing the overall national welfare. For example, the supervisory authorities check the following respects: whether the supervisors understand individual Crypto-Asset Exchange Service Providers' business conditions, management

philosophy, and other particular features and respect Crypto-Asset Exchange Service Providers' initiatives for innovation; and whether Crypto-Asset Exchange Service Providers are not forced to bear undue burdens.

For this quality check, senior officials of both the Strategy Development and Management Bureau and the Supervision Bureau shall verify the supervisory activities from multi-directional perspectives at multiple levels and try to improve supervisory activities on an ongoing basis. The points illustrated below may be checked, taking into account voices from Crypto-Asset Exchange Service Providers.

- When gathering information from Crypto-Asset Exchange Service Providers or having dialogue with Crypto-Asset Exchange Service Providers, effective coordination and information sharing among sector- or area-wise monitoring teams is indispensable in order to eliminate duplication of requests to the Crypto-Asset Exchange Service Providers and to avoid imposing undue burdens on the Crypto-Asset Exchange Service Providers. Is such internal communication and coordination conducted sufficiently? When requesting Crypto-Asset Exchange Service Providers to submit reports or documents, is the content of such request clearly specified? And is due consideration paid to the differences of each Crypto-Asset Exchange Service Provider? Is the submission deadline appropriate to secure sufficient time?
- For accurate profiling, are respective Crypto-Asset Exchange Service Providers' business conditions, management philosophy, and other specific circumstances understood well? Are facts and objective evidential documents used to eliminate the supervisors' preoccupations?
- When identifying priority issues, are individual Crypto-Asset Exchange Service Providers' circumstances fully considered and are substantive issues critical to their business management selected? If there are issues common to multiple Crypto-Asset Exchange Service Providers or industry-wide issues, are those issues detected unfailingly?
- When drawing up a monitoring policy or plan, are appropriate monitoring subjects and methods chosen? Is a system for monitoring established?
- When requesting a Crypto-Asset Exchange Service Provider to submit reports, is the Crypto-Asset Exchange Service Provider fully informed and convinced as to how the supervisors recognize the Crypto-Asset Exchange Service Provider's problems?
- Is dialogue with each Crypto-Asset Exchange Service Provider appropriate in terms of the points mentioned in III-1-3(2)(iii) above? Did the supervisors avoid having the dialogue end up with unilateral administrative guidance?
- Regarding the issues or problems identified through monitoring, are their root causes analyzed?
- In returning the monitoring results, is the most appropriate method selected to focus on priority issues? Does the content of the results clearly describe the points to be discussed or the matters to be improved in accordance with the importance of the matters? Is it free of trivial issues? Is there any content that might unduly interfere with the Crypto-Asset Exchange Service Provider's management?

When returning such results, the supervisory authorities shall endeavor to expand opportunities to receive candid comments and criticisms from Crypto-Asset Exchange Service Providers. For one thing, the supervisors already has a process for inspected firms to file comments on monitoring activities, called the "Inspection Challenge Process." For another thing, senior officials of the supervisory authorities may visit an inspected Crypto-Asset Exchange Service Provider and conduct interviews to seek comments on the monitoring activities directly from the Crypto-Asset Exchange Service Provider's executives and managers.

In addition to the foregoing, the supervisory authorities shall conduct external evaluations of financial administration through interviews with Crypto-Asset Exchange Service Providers and the supervisory

officials, and also invite insights from external experts by such means as holding a panel of experts.

III-1-5 Dealing with Complaints, etc.

(1) Basic response

The Counseling Office for Financial Services Users of the FSA and the relevant division in charge at each Local Finance Bureau shall be the primary contact for receiving consultation and/or complaints, etc. concerning Crypto-Asset Exchange Service Providers. These authorities shall explain to those who made such consultation and complaints, etc. that they are not in a position to conduct mediation, etc. concerning individual transactions and, if necessary, introduce a Designated ADR Body or the Association to them as an institution to respond to such consultation, complaints, etc. pursuant to the law.

If the person who made consultation or complaint, etc. who has given consent to the provision of his/her information to the relevant Crypto-Asset Exchange Service Provider, the supervisory departments shall, in principle, provide relevant information to the Crypto-Asset Exchange Service Provider.

(2) Accumulation of information

Each Local Finance Bureau shall record the content of any consultations, complaints, etc. concerning Crypto-Asset Exchange Service Providers that are deemed to be helpful for supervising Crypto-Asset Exchange Service Providers (Appended Form 2) and, if the information is deemed particularly influential, it shall promptly report it to the relevant division in charge at the FSA.

(3) Cooperation with the Counseling Office for Financial Services Users

To properly reflect feedback from consultation or complaints, etc. received at the Counseling Office for Financial Services Users, the supervisory departments shall take the following measures.

(i) Analysis of details of the inquires and complaints, etc. circulated from the Counseling Office

(ii) Exchange of information with the Counseling Office

(4) Handling of information on a Crypto-Asset that is not necessarily appropriate for Crypto-Asset Exchange Service Providers to handle

In cases where the supervisory departments obtain information from the Association or the like about a Crypto-Asset that is not necessarily appropriate for Crypto-Asset Exchange Service Providers to handle, they shall contact the relevant authorities as necessary.

A Crypto-Asset that is not necessarily appropriate to handle may be determined individually and specifically, for example, by paying attention to the use of the Crypto-Asset (if the Crypto-Asset is clearly being used fraudulently), with reference to “I-1-2-3 judgment Criteria for the Appropriateness of Crypto-Assets Handled.”

III-1-6 Response to Unregistered Business Operators

(1) Grasp of the situations of unregistered business operators or the like

In cases where the supervisory authorities find someone suspected of engaging in the Crypto-Asset Exchange Services without registration (hereinafter referred to as “unregistered business operator or the like”) based on complaints from users, inquiries from the investigative authorities, information provided by Crypto-Asset Exchange Service Providers or the Association, etc., or

advertisements in newspapers and/or on the Internet, the supervisors shall actively strive to grasp the actual situation through inquiries to the police and/or a local consumer affairs center, direct confirmation (regardless of the method of inquiry, such as confirmation by phone or e-mail) with the unregistered business operator or the like.

In particular, when there are complaints, etc. from users or inquiries from the investigative authorities, the supervisors shall not merely respond to them but pay sufficient attention to them.

(2) Handling of unregistered business operators or the like

When having received information concerning an unregistered business operator or the like, the supervisors shall endeavor to take the following measures to prevent the spread of damage.

(i) Receipt of complaints, etc.

Upon receiving information on an unregistered business operator or the like from users, etc., the supervisors shall hear the content of such information (its name, address, name of representative, telephone number, actual conditions of business, name of the applicant, and whether to notify the investigative authorities, etc. of the content of application), and then take the following measures.

(A) When receiving information on an unregistered business operator or the like whose principle place of business is located in the jurisdiction of another Local Finance Bureau, the Local Finance Bureau shall hear the content of information and then notify the Local Finance Bureau having jurisdiction over such business operator (in principle, the latter who is so notified will handle the case).

(B) With regards to a business operator whose contact information is unknown, the supervisors shall endeavor to seek further information.

(C) When requested by an informant not to contact the business operator or other organizations, the supervisors shall take care not to put the informant at a disadvantage.

(D) If the case involves a business operator who is suspected not to have made registration, the supervisors shall suggest that the informant contact and give information to investigative authorities as well.

(E) The supervisors shall prepare "Management ledger (Appended Form 3)" and organize and record the content of complaints and inquiries relating to unregistered business operators or the like and guidance of supervisory authorities to them, and their responses, etc. in chronological order.

(ii) In cases where a business operator is found to be likely to engage in the Crypto-Asset Exchange Services without registration

For a business operator whose name and contact information are known based on information received directly or information provided by the FSA or other bureaus, and whose actual business conditions are also known to some extent, the supervisors shall endeavor to ascertain the actual situation by directly confirming with the unregistered business operator or the like (regardless of the method of inquiry, such as confirmation by phone or e-mail). If, as a result, the business operator is found to be likely to engage in the Crypto-Asset Exchange Services without registration (including the case where the business operator cannot be contacted due to absence, etc.), written inquiries shall be made using Appended Form 5, and the following measures shall be taken.

(A) If the business operator fails to make necessary registration due to lack of intent or malicious intent and is deemed not to have problems from the viewpoint of user protection, the supervisors shall immediately request the business operator to stop the business of

providing Crypto-Asset Exchange Businesses and require the business operator to register as a Crypto-Asset Exchange Service Provider.

(B) If the business operator fails to make necessary registration willingly or with malicious intent and is deemed to have problems from the viewpoint of user protection, the supervisors shall give a written warning in Appended Form 4 to immediately stop such act. In cases where a business operator is found to be clearly engaged in the Crypto-Asset Exchange Services without registration, there is no need to directly confirm with the unregistered business operator or the like or issue the document in Appended Form 5, and the supervisors shall promptly give a written warning in Appended Form 4.

Note: When the supervisors issue a warning in Appended Form 4 or makes an inquiry in Appended Form 5, and if it is deemed necessary for user protection, then the supervisors shall contact the investigative authorities, the relevant ministries and/or governmental agencies, etc.

(iii) Cases where the business operator does not make correction despite of warning

If the business operator does not make correction despite the warning in the Appended Form 4, the supervisors shall file an accusation with the investigative authorities as necessary.

(iv) Publication, etc.

In cases where supervisors have taken a measure such as "warning" or "accusation," the supervisors shall publicize the trade name or person's name (in the case of a juridical person, the name of the representative director or a person equivalent thereto shall be included), location or address (in the case of an individual, the name of the prefecture and the name of the municipality or special ward, and in the case of a non-resident, the name equivalent thereto) of the business operator subject to the measure, as well as the details of the Crypto-Asset Exchange Services provided by the business operator without registration on the website, while copies of the "Management ledger" and "Written warning" etc. shall be promptly sent to the Commissioner of the Financial Services Agency. Upon receiving such report, the FSA shall make a list of such business operators and publish it on the FSA website. In cases where it is difficult to issue a warning letter, such as cases where the address of the business operator subject to the warning is clearly false or where the address of the business operator is unknown, the above-mentioned publication, etc. shall be made without issuing the warning letter.

Note: Cases that would hinder investigations by investigative authorities shall be exempted from any of the responses to unregistered business operators or the like. It should be kept in mind, however, that the fact that the supervisors have received an inquiry about whether the business operator is registered or not from an investigative authorities does not immediately constitute a case that would hinder the investigation by the investigative authorities.

III-1-7 Coordination among Supervisory Departments

(1) Cooperation between the FSA and Local Finance Bureaus

The Financial Services Agency and Local Finance Bureaus need to share awareness of issues deemed necessary for the supervision of Crypto-Asset Exchange Service Providers by appropriately exchanging information. For this reason, the FSA and the Local Finance Bureaus shall make efforts to strengthen the mutual cooperation, such as by providing information in a timely and appropriate manner and exchanging opinions, etc., with regard to information, etc. other than the coordination, etc. pertaining to internal delegated affairs listed in III-1-9, as well.

In addition, the Local Finance Bureaus shall endeavor to strengthen cooperation between themselves by, when they become aware of any undisclosed issues regarding Crypto-Asset Exchange Service Providers supervised by another Local Finance Bureau, providing information to the relevant Local Finance Bureaus or the FSA as appropriate.

(2) Liaison and coordination with the Director-General of the Local Finance Bureau of competent jurisdiction

In the case where an administrative disposition under Article 63-17 of the Act is made to a Crypto-Asset Exchange Service Provider, the details of such disposition shall be promptly notified to the Director-General of another Local Finance Bureau having jurisdiction over the location of the Crypto-Asset Exchange Service Provider's business office.

III-1-8 Cooperation, etc. with Certified Associations for Payment Service Providers

In supervising Crypto-Asset Exchange Service Providers, the supervisors needs to seriously regard the rules made or to be made by Certified Associations for Payment Service Providers (hereinafter collectively referred to as "the Association") in addition to the statutory regulations. The Association also plays an important role in establishing self-regulatory rules, investigating and providing their members with guidance on the compliance with laws and regulations, and resolving complaints from users, among others.

When supervising Crypto-Asset Exchange Service Providers, the supervisors shall pay attention to the following points, given the necessity to ensure appropriate coordination with the Association.

(1) From the viewpoint of conducting efficient and effective supervision of Crypto-Asset Exchange Service Providers who are members of the Association, the supervisors shall hold an interview as needed with regard to the investigations, audits, and guidance for improvement, etc. (including examination findings concerning the screening of the appropriateness of a Crypto-Asset) conducted by the Association for its members.

(2) For minor matters that are not necessarily in violation of laws and regulations and for which it is deemed appropriate and effective for the Association to provide improvement guidance, etc., the supervisors may, in close cooperation with the Association, request the Association to give improvement guidance, etc. and to pay attention to such matters in its investigation, while taking into consideration the supervisory right of the authorities.

(3) With regard to complaints, etc. received by the Association and the status of processing complaints and the trend of the complaints, the supervisors shall regularly hold an interview and exchange opinions with the Association.

(4) From the perspective of supervising Crypto-Asset Exchange Service Providers including non-members appropriately and efficiently, the supervisory authorities shall closely cooperate with the Association with regard to the establishment, amendment, and status of operation of the self-regulatory rules.

For example, from the viewpoint of protecting users, it is desirable to establish specific guidelines for separate management and Crypto-Asset margin trading in the self-regulatory rules.

III-1-9 Internal Delegation

(1) Coordination with the Commissioner of the Financial Services Agency

The Director-General of the Local Finance Bureau shall, in processing the matters to be delegated to him/her regarding supervisory affairs of Crypto-Asset Exchange Service Providers, coordinate in advance with the Commissioner of the FSA with regard to the following matters (which does not preclude the coordination with the Commissioner of the FSA with other matters on an as-needed basis). It should be noted that, at the time of coordination, the Director-General of a Local Finance Bureau shall report the results of the deliberations made by his/her bureau (including deliberations made pursuant to III-3(3) hereof) and express the opinions thereof.

(i) Order to improve business operations under Article 63-16 of the Act

(ii) Revocation of registration or business suspension based on Article 63-17(1) of the Act

(2) Sub-delegation to the Head of Local Finance Office, etc.

In cases where the location of the headquarters (referring to the "headquarters" stipulated in Article 8 of the Cabinet Office Order; the same shall apply hereinafter) of an applicant for registration and a Crypto-Asset Exchange Service Provider is within the jurisdictional district of a Local Finance Office, the Otaru Sub-office of Hokkaido Local Finance Bureau, or the Kitami Sub-office of Hokkaido Local Finance Bureau, the authorities delegated to the Director-General of a Local Finance Bureau pertaining to the acceptance of written notification, applications, and reports submitted by the applicant for registration or the Crypto-Asset Exchange Service Provider may be delegated to the Head of said Local Finance Office or Sub-Office.

The written notifications, etc. concerning these matters shall be submitted to the attention of the Director-General of the Local Finance Bureau having jurisdiction over the location of the headquarters of an applicant for registration or a Crypto-Asset Exchange Service Provider.

III-2 Various Administrative Procedures

III-2-1 Application for Registration and Acceptance of Notification

Administrative processes pertaining to applications for the Crypto-Asset Exchange Services registration and changes thereof, as well as public inspection of such registers shall be handled as follows.

(1) Acceptance of application for registration and notification

(i) When accepting an application for registration and/or notification of change thereof, the supervisors shall pay attention to the following matters and, if finding them inappropriate, request the Crypto-Asset Exchange Service Provider who submitted the application and/or notification to make a correction.

(A) The applicant must not use any trade name or name that is likely to mislead users to think that it is a public institution or a financial institution or that it has a special relationship therewith, or to impair the fairness of transactions.

(B) The applicant must not make two or more applications for registration using two or more trade names.

(C) The following matters shall be stated in any entrustment agreement to be submitted pursuant to Article 6 (xvi) of the Cabinet Office Order.

a) The entrustee's obligation to comply with the Payment Services Act

b) Matters concerning the scope of entrusted operations;

c) Matters concerning how to determine and how to pay the commission to entrustees;

d) Sharing of expenses necessary for handling the entrusted operations; and

e) Entities to install business facilities and equipment

(ii) The contents of "documents explaining the outline of Crypto-Assets" as provided in Article 6(xi) of the Cabinet Office Order shall be in accordance with the forms, etc. separately published by the Association.

(iii) With regard to "documents containing other reference information" prescribed in Article 6 (xviii) of the Cabinet Office Order, the following documents must be attached to the written application for registration, for example.

(A) "Questionnaire on Registration Screening of Crypto-Asset Exchange Service Providers"

(B) Document stating the quantity of Performance Guarantee Crypto-Assets for one business year after the commencement of business pertaining to the Crypto-Asset Exchange Services and the estimated amount in yen terms when the quantity is converted into the Japanese currency

(iv) The "place where the principal activities in the course of the business of the Crypto-Asset Exchange Services are carried out" as set forth on page 3 of Appended Form 1 of the Cabinet Office Order and on page 4 of Appended Form 2 of the Cabinet Office Order refers to the place where important business operations are carried out for transactions pertaining to the Crypto-Asset Exchange Services with users, such as Exchange of Crypto-Assets, etc. or management of users' money and their Crypto-Assets, etc.

(2) Examination of applications for registration

When screening applications for registration (including prior consultations; the same shall apply hereinafter), the supervisors shall conduct in-depth screening with a focus on substances, based on the "Screening Procedure for Applications for Registration of Crypto-Asset Exchange Service Providers" (see the FSA website).

Specifically, the supervisors shall confirm, in writing and with evidence, the business plan of each applicant business operator and its effective internal control environment in accordance with the plan, as well as the development status of a governance framework with its priority on user protection, carry out an onsite-visit verification, and hold an interview with its officers. On such occasions, the supervisors shall utilize the "Questionnaire on Registration Screening of Crypto-Asset Exchange Service Providers," which supplements and extends the supervisory viewpoints in these Guidelines and is a tool to facilitate dialogue with these business operators.

(i) The regulators shall assess the financial foundation under Article 63-5(1)(iii) of the Act in accordance with the following.

Note: When assessing the following matters, the supervisors shall conduct interviews about the method of management of users' property as prescribed in Article 63-11 of the Act, based on the details of "Content and Method of the Crypto-Asset Exchange Services" included in the written application for registration, the latest balance sheet, etc. as prescribed in Article 6(viii) of the Cabinet Office Order, the "document stating the expected income and expenditures pertaining to the Crypto-Asset Exchange Services for the first three business years after the commencement of the business" as prescribed in Article 6(x) of the Cabinet Office Order, and the details of the "internal rules, etc. concerning the Crypto-Asset Exchange Services" as prescribed in Article 6(xiv) of the Cabinet Office Order.

(A) For a newly established organization, its financial foundation shall be assessed based on its balance sheet at the time of the establishment.

(B) When confirming the content of the "the latest balance sheet (including the related notes)

and profit and loss statement (including the related notes) or any substitute thereof" under item (viii) of Article 6 of the Cabinet Office Order in the case where the applicant does not hold the documents (audit certificate) under item (ix) of said Article, the following documents, for example, shall be used as necessary.

a) If savings are recorded, a certificate of the balance issued by a financial institution who trades with the applicant;

b) In cases where securities are recorded, a report on the balance of transactions issued by a securities company who trades with the applicant;

c) In cases where land or buildings are recorded, a copy of fixed asset valuation certificate issued by a municipality or appraisal report prepared by a real estate appraiser;

d) A copy of a tax return from for corporation tax and a copy of the balance sheet attached thereto.

(C) Regarding the prospective income and expenditures, the supervisors shall confirm whether the applicant business operator has established plans and measures to cope with deterioration of the business environment such as the entry of any competitor or the system obsolescence, and whether the plan anticipates a certain level of earnings even under such a scenario. In addition, if there are special circumstances that are considered to affect the continuity of the Crypto-Asset Exchange Services, such as a case where any loss incurred in the Crypto-Asset Exchange Services can be offset by earnings from other businesses operated by the applicant, the supervisors shall consider such circumstances.

(D) In cases where an applicant business operator intends to manage Crypto-Assets, the amount of net assets is required "to be at least equivalent to the amount that is obtained by converting the quantity of Performance Guarantee Crypto-Assets into the Japanese currency" as provided for in Article 9(1)(ii) of the Cabinet Office Order. When confirming whether this requirement is met, the examiner shall, based on the respective contents of the documents set forth in (1)(ii)(B) above, first examine whether the estimated quantity of Performance Guarantee Crypto-Assets for one business year after the commencement of business pertaining to the Crypto-Asset Exchange Services is reasonable in light of the business plan of the business operator, and then confirm whether the amount of its net assets exceeds the amount that is obtained by converting the estimated quantity of the Performance Guarantee Crypto-Assets into the Japanese currency.

(ii) In examining whether the applicant falls under the category of a "corporation which has not established a system to ensure the proper and secure conduct of the Crypto-Asset Exchange Services" as prescribed in Article 63-5(1)(iv) of the Act and the category of a "corporation which has not established a system that is necessary for ensuring compliance with the provisions of this Chapter" as prescribed in Article 63-5(1)(v) of the Act, the examiner shall pay attention to the following points.

(A) Has the applicant established a control environment to appropriately respond to major supervisory viewpoints listed in II-1 and II-2, for example, regarding cross-border transactions, or whether cash acceptance/payment is involved or not, in light of the contents of business of the Crypto-Asset Exchange Service Provider, and its business plan (Including its scale and characteristics)?

In particular, when confirming the organizational structure, has the applicant developed internal control environment (including an internal audit structure suited to the nature of business) in which the mutual check function effectively works, including the structure for legal compliance?

(B) Do the articles of incorporation include the operation of the Crypto-Asset Exchange Services as a corporate purpose?

(C) Expertise is required for judging the appropriateness of the handling of Crypto-Assets as provided for in Article 6(xi) of the Cabinet Office Order. On top of that, there are some fraudulent Crypto-Assets. In this context, does the applicant take into account information provided by other Crypto-Asset Exchange Service Providers and the Association, etc. and appropriately assess whether the handling of the Crypto-Assets listed in II-2-2-1-2(4) is appropriate or not, (including the review after start of the handling)?

(D) With regard to the matters prescribed in Article 6(xv) of the Cabinet Office Order, does the content of the submitted application take into consideration the matters prescribed in each item of Article 22(1) to (4) of the Cabinet Office Order?

(iii) When assessing whether a business operator who does not plan to join the Association at the time of registration application is "a corporation that has not prepared internal rules that have contents equivalent to the articles of incorporation or other rules of the Certified Association for Payment Service Providers or has not established a system for ensuring compliance with those internal rules" as prescribed in Article 63-5(1)(vi) of the Act, such assessment shall be based on II-4-2. Meanwhile, the business operator shall be notified of the following matters and shall be requested to take appropriate measures.

(A) If, after the registration, the business operator has not prepared internal rules that have contents equivalent to the Association Rules or has not established a system for ensuring compliance with those internal rules, supervisory measures shall be taken in accordance with II-4-3.

(B) If the internal rules are not reviewed in accordance with the revision, etc. of the Association Rules, it may fall under (A) above.

(3) Processing of applications for registration

(i) A written notice of completion of registration under Article 7 of the Cabinet Office Order shall be treated as follows.

(A) The registration number shall be assigned serially from 00001 in the order of completion of approvals by the Directors-General of Local Finance Bureaus.

(B) When a registration is no longer valid, its registration number shall be retired and no replacement shall be made.

(C) With regard to a notification for change of the location of the headquarters, which is beyond the jurisdictional district of the local finance bureau, its registration number shall be newly given by the Director-General of the Local Finance Bureau who effected the new registration in serial in accordance with (A) above.

(ii) If a registration is refused, a written notice of refusal of registration, stating the reasons for refusal, etc., based on Article 10 of the Cabinet Office Order shall be delivered to the registration applicant (See III-4).

(iii) When refusing the registration, the Director-General of the Local Finance Bureau shall notify the Director-General of the Supervisory Bureau of the FSA to that effect by sending a written notice of refusal of registration of the Crypto-Asset Exchange Service Provider using Appended Form 6 together with a copy of the written application for registration.

(4) Processing of the notification of change

(i) If it becomes clear that a person newly appointed as an officer of the notifier falls under any

of Article 63-5(1)(xi)(a) through (e) of the Act, the supervisory authorities shall take measures such as revocation of registration prescribed in Article 63-17 of the Act with respect to the notifier.

(ii) As for "cases where a new Crypto-Asset is granted to the holder of an existing Crypto-Asset due to a change in the technology or specifications used for the existing Crypto-Asset handled" prescribed in Article 11(ii) of the Cabinet Office Order, a conceivable case, for example, is that, when a new Crypto-Asset arises due to branching of the blockchain used for an Entrusted Crypto-Asset, a Crypto-Asset Exchange Service Provider grants the new Crypto-Asset to the holder of the Entrusted Crypto-Asset in relation to its Crypto-Asset Exchange Services.

Note: It should be kept in mind that in cases where a Crypto-Asset Exchange Service Provider comes to know in advance the fact of branching of the blockchain, etc. in connection with its business operation for the Crypto-Asset Exchange Services, the Crypto-Asset Exchange Service Provider is required to make an advance notification of change based on Article 63-6(1) of the Act.

(iii) "Matters equivalent thereto" as prescribed in Article 11(iii)(a) of the Cabinet Office Order refers to cases where there is no change in the type of the Crypto-Asset Exchange Services itself, but there is a material change in the contents and method of the business operation. Such cases, for example, include changes in the contents of the business operation that involve a change in the business model.

Note: Changes in the contents of the business operation involving a change in the business model may include, for example, the addition of a new business to sell tokens issued in ICOs to users at the request of these issuers, in addition to the current business of selling to users Crypto-Assets procured from the counterparty of proprietary cover trading.

(iv) In cases where the change so notified is a change of the location of the headquarters beyond the jurisdictional district of the Local Finance Bureau, such change shall be treated as follows.

(A) The Director-General of the Local Finance Bureau who receives the notification of change of registered matters shall retain the attached documents under Article 12(2)(ix) of the Cabinet Office Order (the written notice of completion of registration).

(B) The Director-General of the Local Finance Bureau who has received the relevant notification of change under (A) above shall notify the Director-General of the Local Finance Bureau who will newly have the authority of registration pursuant to Article 12(3) of the Cabinet Office Order with the written notification of change prepared using Appended Form 7, together with a copy of the relevant notification of change, the part of the register of Crypto-Asset Exchange Service Providers relating to the notifier, the written opinion of the Local Finance Bureau prepared using Appended Form 8, the previous written application for registration and documents to be attached thereto, as well as a copy of the report on the inspection conducted immediately prior to the submission of the relevant notification of change.

(C) The Director-General of the Local Finance Bureau to whom the written notification described in (B) above has been sent shall, without delay, register the relevant information in the register of Crypto-Asset Exchange Service Providers and notify the Director-General of the Local Finance Bureau who previously registered the information through the written notice of completion of registration of change prepared using Appended Form 9.

(5) Issuance of certificates of registration

If a registered Crypto-Asset Exchange Service Provider or a person who was a Crypto-Asset Exchange Service Provider files an application for the registration certificate for the reason that it is necessary to submit it to a public institution, the regulators shall issue a certificate of registration for the Crypto-Asset Exchange Service Provider pursuant to Appended Form 10. Provided, however, that this shall not apply to cases where the registration application documents have already been disposed of after the expiration of the retention period.

(6) Preparation of the register of Crypto-Asset Exchange Service Providers

Based on the written application for registration prescribed in Article 4 of the Cabinet Office Order (pages 2 to 13 of Appended Form 1 of the Cabinet Office Order, (in the case of a foreign Crypto-Asset Exchange Service Provider, pages 2 to 14 of Appended Form 2 of the Cabinet Office Order)), the registry pertaining to the registered Crypto-Asset Exchange Service Provider shall be organized by the Crypto-Asset Exchange Service Provider and kept in the register.

(7) Public inspection of the register of Crypto-Asset Exchange Service Providers

Public inspection of the register of Crypto-Asset Exchange Service Providers under Article 8 of the Cabinet Office Order shall be treated as follows.

(i) A person who made a request for public inspection shall be required to fill in the prescribed items on the application for public inspection of the register of Crypto-Asset Exchange Service Providers pursuant to Appended Form 11. Note that a person who has changed his/her surname may additionally enter his/her former surname (which refers to the "former surname" prescribed in Article 30-13 of the Order for Enforcement of the Residential Basic Book Act (Cabinet Order No. 292 of 1967); the same shall apply in II-2-5) and his/her given name in brackets in the "name of applicant" column.

(ii) The date and time of inspection of the register shall be as follows.

(A) The date of public inspection shall be days other than Saturdays, Sundays, holidays prescribed in Article 3 of the Act on National Holidays, January 2 and 3, and from December 29 to 31.

(B) The public inspection time shall be within the time specified by the Director-General of the Local Finance Bureau.

(C) When it is necessary to organize the register, etc. or for any other reason, the public inspection date or time may be changed.

(iii) The register, etc. may not be taken out of the place of the public inspection designated by the Director-General of the Local Finance Bureau.

(iv) The following persons may be suspended or refused for public inspection:

(A) Any person who fails to follow (i) through (iii) above or the instructions of the staff

(B) Any person who has damaged or is deemed likely to damage the register, etc.

(C) Any person who has caused or is deemed likely to cause trouble to others.

III-2-2 Written Reports under Article 63-14 of the Act

(1) Written Reports under Article 63-14(1) of the Act

When processing business reports set forth in Appended Form 11 of the Cabinet Office Order (in the case of a Foreign Crypto-Asset Exchange Service Provider, Appended Form 12 of the Cabinet Office Order), the following points shall be taken into consideration.

(i) After reviewing the reporting contents with reference to the matters confirmed at the time of

application for registration, such as the management plan and financial plan, if there is a significant discrepancy between the two, the supervisors shall confirm the actual business conditions through interviews with the Crypto-Asset Exchange Service Provider.

(ii) If, as a result of confirming the actual business conditions, there is a potential of "lacking a sufficient financial foundation that satisfies the requirements specified by Cabinet Office Order as those found to be necessary for the proper and secure conduct of the Crypto-Asset Exchange Services" stipulated in Article 63-5(1)(iii) of the Act, the supervisors shall consider necessary measures, such as collecting a report based on Article 63-15 of the Act.

(2) Written reports under Article 63-14(2) of the Act

The following points shall be taken into consideration when processing a report on the management of Users' Property prescribed in Appended Form 13 of the Cabinet Office Order.

(i) In cases where the amount of money, the quantity of Crypto-Assets, or the appraised value of any Crypto-Asset has significantly changed, the supervisors shall confirm the reason for such change and the prospects for future changes, etc. through interviews or other means.

(ii) In cases where a Crypto-Asset Exchange Service Provider manages Crypto-Assets, the supervisors shall check, with reference to the latest financial statements, etc., whether or not the amount of net assets of the Crypto-Asset Exchange Service Provider falls below the amount that is obtained by converting the quantity of Performance Guarantee Crypto-Assets into the Japanese currency.

(3) Sending to the FSA, etc.

(i) Occasional reporting related to Crypto-Asset Exchange Service Providers

A duplicate copy of the report on the management of Users' Property and a copy of each reference document, as well as a written opinion with regard to (1) or (2) above, if any, shall be sent to the relevant department in charge at the FSA within one month after the deadline for submission.

(ii) Periodic reporting related to Crypto-Asset Exchange Service Providers

(A) The Director-General of the Local Finance Bureau shall collect from each Crypto-Asset Exchange Service Provider its business report as of the end of March every year prepared using Appended Form 12, with the deadline being the end of May every year, pursuant to Article 63-15(1) of the Act.

(B) A copy of the business report of each Crypto-Asset Exchange Service Provider shall be sent to the relevant department in charge at the FSA by the end of June every year.

(iii) Submission of a list of registration status of the Crypto-Asset Exchange Services

(A) A list of registration status for all registered Crypto-Asset Exchange Service Providers shall be updated for each registration and sent to the Director-General of the Supervisory Bureau of the FSA within 20 days after the end of each six-month period.

(B) The list must always include the following;

- Name of each registered Crypto-Asset Exchange Service Provider
- Registration No.
- Registration date
- Date of closure
- Phone number and e-mail address of the Crypto-Asset Exchange Service Provider
- Name of each Crypto-Asset to be handled
- Type of by-business

III-2-3 Response to Cases Where Property Requirements Are Not Satisfied

In cases where the amount of net assets of a Crypto-Asset Exchange Service Provider has fallen below the Minimum Net Assets during the registration period, the supervisory authorities shall take the following measures in view that the Crypto-Asset Exchange Service Provider may be subject to the disposition of rescinding the registration, etc. pursuant to Article 63-17(1)(i) of the Act.

(1) In cases where a Crypto-Asset Exchange Service Provider is found not to satisfy the property requirements through the confirmation described in III-2-2(2)(ii), the supervisory authorities shall request the Crypto-Asset Exchange Service Provider to make a report on the following details, pursuant to Article 63-15 of the Act.

(A) Amount of net assets

(B) Amount that is obtained by converting the quantity of Performance Guarantee Crypto-Assets into the Japanese currency (only for the case where the Crypto-Asset Exchange Service Provider manages Crypto-Assets)

(C) Grounds for calculation of (A) and (B) above

(D) Plan to restore the net assets

Note: If the appropriateness of the amount of net assets described in (A) above is doubted, in light of generally accepted accounting practices, the supervisors shall request the Crypto-Asset Exchange Service Provider to report about its opinion and the grounds for calculation, etc.

(2) If the report as described in (1) above is submitted, the supervisors shall examine the validity of the reporting contents. In particular, the supervisors shall thoroughly examine the feasibility of the "plan to restore net assets." If the examination findings suggest that the plan is deemed to be capable of restoring the net assets promptly and reliably, the disposition shall be withheld and the supervisors shall follow up the implementation status of the plan through interviews or collecting reports.

(3) If the examination findings suggest that the Crypto-Asset Exchange Service Provider is unlikely to satisfy the property requirements, the disposition of revoking the registration, etc. shall be rendered pursuant to Article 63-17 of the Act. (Provided, however, that this shall not apply to cases where the Crypto-Asset Exchange Service Provider goes or already went out of business.)

III-2-4 Treatment of Discontinuation, etc.

(1) In cases where a Crypto-Asset Exchange Service Provider submits a notification of discontinuation, etc. of the Crypto-Asset Exchange Services (hereinafter referred to as the "notification of discontinuation, etc.") pursuant to Article 63-20 of the Act, or in cases where the registration of a Crypto-Asset Exchange Service Provider has been revoked pursuant to Article 63-17(1) of the Act, the supervisors shall request the Crypto-Asset Exchange Service Provider to report, by using Appended Form 13, about the amount of liabilities borne in relation to Exchange of Crypto-Assets, etc. and relevant information based on Article 63-15 of the Act.

Note 1: It should be kept in mind that if a notification of discontinuation, etc. of part of the Crypto-Asset Exchange Services is submitted pursuant to Article 63-20(1) of the Act, only the Crypto-Asset Exchange Services pertaining to said discontinued business will be subject to the amount of liabilities borne in relation to Exchange of Crypto Assets, etc. prescribed in Article 63-20(5) of the Act.

Note 2: The "discontinuation of part of the Crypto-Asset Exchange Services" prescribed in Article 63-20(1)(i) of the Act refers to, for example, cases where a Crypto-Asset Exchange Service Provider dealing in multiple Crypto-Assets discontinues dealing in some of such Crypto-Assets, or cases where a Crypto-Asset Exchange Service Provider providing Crypto-Asset-based multiple services discontinues part of such services.

(2) In cases where a report set forth in (1) above has been submitted, the supervisors shall order, based on Article 63-15 of the Act, the Crypto-Asset Exchange Service Provider to report without delay to the effect that it has completed the performance of liabilities borne in relation to Exchange of Crypto-Assets, etc. that it intended to discontinue as part of the Crypto-Asset Exchange Services upon said completion, or to that effect it has changed its contact information or its trade name before the completion, if any. In addition, when it is necessary to protect users, the supervisors shall order the Crypto-Asset Exchange Service Provider to periodically report its performance status of the obligations.

(3) In cases where a Crypto-Asset Exchange Service Provider has submitted the notification of discontinuation, etc. pursuant to Article 63-20(1)(i) of the Act (limited to cases where said business was succeeded through transfer of business, merger or company split, or for other reasons), the Director-General of a Local Finance Bureau who has received said written notification of discontinuation, etc. shall send the notice of business transfer prepared by using Appended Form 14 together with said notification of discontinuation, etc. a copy of the portion of the register of Crypto-Asset Exchange Service Providers pertaining to said notifier, and the report on the management of Users' Property for the immediately preceding Base Date to the Director-General of a Local Finance Bureau who has accepted or registered the notification of another Crypto-Asset Exchange Service Provider to which said business is transferred.

(4) The Director-General of the Local Finance Bureau to which the written notice described in (3) above has been sent shall, without delay, confirm whether necessary measures, including the submission of a written notification of change pertaining to the business, have been taken with regard to the Crypto-Asset Exchange Service Provider to which the relevant business has been transferred.

III-2-5 Points of Attention regarding Statements in Reports Submitted by Crypto-Asset Exchange Service Providers

For the entry of names in a series of the appended forms, a person who additionally entered his/her former surname and given name in brackets in either the written application for registration or the notification of change may additionally enter his/her former surname and given name either in brackets or in lieu of his/her full name.

III-2-6 Points of Attention regarding Written and Face-to-Face Procedures

An application and notification to be submitted by a Crypto-Asset Exchange Service Provider, etc. to competent authorities and a disposition notice, etc. to be issued by the competent authorities to a Crypto-Asset Exchange Service Provider, etc. may be made by using an electronic data processing system pursuant to Article 6(1) and Article 7(1) of the Act on Promotion of Administration by Use of Information and Communications Technology (hereinafter referred to as "Digital Procedure Act"), even if any other laws and regulations stipulate that such application, notification, etc. and disposition

notice, etc. shall be made in writing, etc., or by other methods.

In light of the purpose of the Digital Procedures Act, the provisions of these Guidelines related to procedures covered by the Digital Procedures Act may also be fulfilled by means of an electronic data processing system, regardless of the provisions requiring a written or face-to-face means.

In addition, while digitization is rapidly advancing in all economic and social activities, the Government as a whole is reviewing Japan's systems and practices based on written, stamped, and face-to-face procedures, and is moving forward with efforts toward the realization of a remote society in which procedures can be carried out without actually having to travel.

In order to steadily advance these efforts, the FSA has also promoted the computerization of administrative procedures by updating the FSA Electronic Application and Notification System, which enables online submission of all procedures for applications and notifications received from Crypto-Asset Exchange Service Providers, etc. and by revising Cabinet Office Orders and supervisory guidelines to abolish seals.

Furthermore, with regard to procedures between private business operators, as well, the FSA established the "Panel for Reviewing Procedures Requiring Documents, Seals, and Face-to-Face Contact in the Financial Industry" to encourage the industry as a whole to review conventional practice and has made efforts to promote digitalization of documents, to eliminate the seal procedures and to review face-to-face requirements.

In light of such efforts by the public and private sectors, written and/or face-to-face requirements in these Guidelines other than those related to procedures covered by the Digital Procedure Act may also be fulfilled by means of an electronic data processing system or other information and communications technology, except for cases where the submission of an original document is required in III-2-7 hereof.

Considering the intent of the abovementioned handling, the FSA and relevant supervisory authorities shall promote conduct of procedures based on the provisions of these Guidelines in a manner other than in writing or in person, whenever possible, taking into account the intentions of the parties to the procedures.

III-2-7 Points of Attention when Submitting Applications etc.

Based on III-2-6 hereof, the FSA and relevant supervisory authorities shall require, in principle, that applications and/or notifications by Crypto-Asset Exchange Service Providers, etc. be submitted by the deadline specified by relevant laws and regulations using the FSA Electronic Application and Notification System.

However, as for any of the attached documents (a copy of certificate of residence, an identification card, a copy of family register, documents certifying payment of taxes/fees, etc.) issued by public institutions, the original thereof is required to be sent.

For the time being, e-Gov on the website of the FSA is also available for submission of notifications, applications, or other procedures that are allowed to be processed through e-Gov, in parallel with the FSA Electronic Application and Notification System.

III-3 Points of Attention in Enforcing Administrative Dispositions

Major adverse dispositions (as defined in Article 2(iv) of the Administrative Procedure Act; the same shall apply hereinafter) enforced by supervisory authorities include: (i) the issuance of an order to improve business operations under Article 63-16 of the Act, (ii) the issuance of a business suspension order under Article 63-17 of the Act, and (iii) the revocation of a registration under Article 63-17 of the Act. The basic workflow for rendering such administrative dispositions is illustrated as follows.

(1) Order to submit reports pursuant to Article 63-15 of the Act

(i) If the on-site inspection or off-site monitoring (such as interviews or demanding submission of a misconduct notification) finds out any problem in compliance management systems, governance systems, or other business practices of the inspected Crypto-Asset Exchange Service Provider, the supervisors shall ask the Provider to report its fact-checking of the problems, its own analyses of the causes of those problems, planned measures for improvement or remediation, and other necessary matters pursuant to Article 63-15(1) of the Act.

(ii) If the supervisors determine, as a result of verifying the report submitted by the Crypto-Asset Exchange Service Provider, that further scrutiny is needed, the supervisors shall ask it to submit an additional report pursuant to Article 63-15(1) of the Act.

(2) Follow-up on measures for improvement or remediation reported under Article 63-15(1) of the Act

(i) If the supervisors determine, as a result of verifying the reports submitted by a Crypto-Asset Exchange Service Provider, that no serious issue is found in terms of the soundness and appropriateness of its business and that the Crypto-Asset Exchange Service Provider is capable of promoting its self-initiated improvement efforts, the supervisors shall follow up on the progress of its measures for improvement reported in (1) above through non-compulsory interviews or other communication.

(ii) If necessary, the supervisors may ask the Crypto-Asset Exchange Service Provider to make periodic follow-up reports pursuant to Article 63-15(1) of the Act.

(3) Order to improve business operations, order to suspend business, or revocation of registration based on Article 63-16, or Article 63-17(1) of the Act

If the supervisors determine, as a result of verifying the relevant reports (including the additional reporting) as its response to inspection results or off-site monitoring, etc., that a serious issue is found concerning the protection of the interests of users, etc., it will take into account the factors listed in (1) to (3) below, examine whether there are any other factors to be considered, and then consider the following issues, and ultimately determine the content of the final administrative disposition.

- Whether it is appropriate to leave initiatives for improvement to voluntary efforts of the Crypto-Asset Exchange Service Provider;
- Whether it needs considerable efforts for the improvement and whether the Crypto-Asset Exchange Service Provide needs to focus on the business improvement for a certain period of time; and
- Whether it is appropriate for the Crypto-Asset Exchange Service Provide to continue the business;

(Blank)

(i) Severity and maliciousness of the misconduct

(A) Degree of detriment to public interests

Does the Crypto-Asset Exchange Service Provider substantially infringe on the public interest by seriously impairing the credibility of Crypto-Asset Exchange Services?

(B) Degree of damage to users

Do a large number of users in extensive areas suffer damage? How serious is each user's damage?

(C) Maliciousness of the improper conduct
For example, with regard to reporting on the management of Users' Property, did the Crypto-Asset Exchange Service Provider commit a malicious conduct, such as making a false report?

(D) Duration of the improper conduct and its repetitions
Has the conduct in question been continued over a long time or for a short period? Was it committed repeatedly or continuously? Or only once? Had the Crypto-Asset Exchange Service Provider committed any similar violation in the past?

(E) Intentionality
Did the Crypto-Asset Exchange Service Provider intentionally act with an awareness of illegality or inappropriateness? Or was it mere negligence?

(F) Institutional involvement
Was the conduct in question at the sole discretion of a person in charge or based on directions from a high-level officer? Were the management team of the Crypto-Asset Exchange Service Provider involved in the conduct?

(G) Attempt to cover up the improper conduct
After the Crypto-Asset Exchange Service Provider or the persons in charge had recognized the problem, did they attempt to conceal its evidence? If so, was it an institutional attempt?

(H) Involvement of anti-social forces
Were any anti-social forces involved in the conduct in question? If so, to what extent were they involved?

(ii) Appropriateness of governance systems and business operation frameworks leading to the causes of the improper conduct

(A) Is the management team of the Issuer of Prepaid Payment Instruments fully aware of the significance of compliance and eager to promote compliance-conscious management?

(B) Is the Internal Audit Department of the Crypto-Asset Exchange Service Provider well prepared? Does it exert its functions properly?

(C) Are the Crypto-Asset Exchange Service Provider's Compliance Department and Internal Control Department well prepared? Do they exert their functions properly?

(D) Are relevant staff of the Crypto-Asset Exchange Service Provider fully aware of the significance of compliance? Are they adequately trained or educated?

(iii) Mitigating factors
In addition to (i) and (ii) above, are there any factor that can allow the supervisory authorities to mitigate administrative enforcement? For example, is the Crypto-Asset Exchange Service Provider promoting self-initiated efforts for protecting users, etc. before receiving any administrative measure?

(4) Standard period for processing a case subject to administrative disposition
Supervisory dispositions pursuant to Article 63-16 or Article 63-17(1) of the Act, if any, shall be given within approximately one (1) month (or approximately two (2) months if coordination with the FSA is required, in principle, from the time of receipt of the report described in (1) above.

Note 1: The following points should be taken into consideration in determining "the time of receipt of the report".

(A) If asking for submission of a report multiple times pursuant to Article 63-15(1) of the Act (limited to the case where each request for submission is made within the time frame specified above after receiving the immediately preceding report), the time for receiving

the last report is regarded as the starting point of the time frame for administrative disposition.

(B) If asking for correction of a report submitted or for submission of additional documents (excluding inconsequential correction or provision of trivial information), the time for receiving corrected or additional documents is regarded as the starting point of the time frame for administrative disposition.

Note 2: The time spent for formal explanations or hearings is not included in the standard period for processing a case subject to administrative disposition.

Note 3: The standard period for processing a case subject to administrative disposition will apply to each set of information to be examined as the basis for invoking administrative disposition.

(5) Cancellation of the obligation to make progress reports based on the order to improve business operations issued under Article 63-16 of the Act

After issuance of an order to improve business operations to a Crypto-Asset Exchange Service Provider under Article 63-16 of the Act, the supervisors shall, in principle, ask the Crypto-Asset Exchange Service Provider to report the progress of its business improvement plan so that the supervisors can follow up on the approach of the Crypto-Asset Exchange Service Provider for business improvement based on such order and encourage its improvement efforts. For this, the following points shall be taken into consideration.

(i) If the supervisors ask a Crypto-Asset Exchange Service Provider to which it has issued an order to improve business operations pursuant to Article 63-16 of the Act to submit a report on the progress of the business improvement plan within a limited period, the Crypto-Asset Exchange Service Provider shall be relieved of the obligation to make a report after expiration of the specified period.

(ii) If the supervisors ask a Crypto-Asset Exchange Service Provider to which it has issued an order to improve business operations pursuant to Article 63-16 of the Act to submit a report on the progress of the business improvement plan on an going basis without specifying a definite period, the supervisors shall cancel the obligation of the Crypto-Asset Exchange Service Provider to make a report when the supervisors determine that adequate improvement measures have been completed in line with the business improvement plan to address the problem triggering the order to improve business operations. In this regard, the supervisors determine whether or not to cancel the obligation of the Crypto-Asset Exchange Service Provider to submit a report by evaluating its improvement efforts reported by the Crypto-Asset Exchange Service Provider or confirmed through the supervisor's inspections.

III-4 Relationship with the Administrative Procedure Act and Other Relevant Acts

(1) Relationship with the Administrative Procedure Act

When the supervisors intend to render any adverse disposition falling under any of the cases set forth in Article 13(1)(i) of the Administrative Procedure Act to a Crypto-Asset Exchange Service Provider, the supervisors must conduct hearings with the Crypto-Asset Exchange Service Provider. In case of any adverse disposition falling under the case set forth in item (ii) of the same paragraph, the supervisors must offer the opportunity for explanation to the Crypto-Asset Exchange Service Provider.

In either case, the supervisors must show the grounds for the adverse disposition pursuant to Article 14 of the same Act. (When such adverse disposition is rendered in writing, its grounds

must also be indicated in writing.)
If intending to refuse to grant the permission, license, or other approval requested under an application filed by a Crypto-Asset Exchange Service Provider, the supervisors must show the grounds for the disposition of refusal pursuant to Article 8 of the same Act. (When such disposition is rendered in writing, its grounds must also be indicated in writing.)
On this occasion, merely enumerating the provisions of relevant acts is not sufficient; instead, full accountability is required to clarify what facts underlie the decision to render the disposition and which acts and standards are relied on to justify the disposition.

(2) Relationship with the Administrative Complaint Review Act
If the supervisors intend to render any disposition against which a complaint may be filed, it should be kept in mind that the supervisors must explain in writing that the Crypto-Asset Exchange Service Provider is entitled to file a complaint pursuant to Article 82 of the Administrative Complaint Review Act (Act No. 68 of 2014).

(3) Relationship with the Administrative Case Litigation Act
If the supervisors intend to render any disposition against which an action for revocation may be filed, it should be kept in mind that the supervisors must explain in writing that the Crypto-Asset Exchange Service Provider is entitled to file a lawsuit pursuant to Article 46 of the Administrative Case Litigation Act (Act No. 139 of 1962).

III-5 System for Exchange of Opinions

Before rendering any adverse disposition to a Crypto-Asset Exchange Service Provider, the supervisors are supposed to conduct hearings with the Crypto-Asset Exchange Service Provider or give an opportunity for explanations to the Crypto-Asset Exchange Service Provider in accordance with the Administrative Procedure Act. In addition to and apart from such hearings or explanations, there is a system to allow the Crypto-Asset Exchange Service Provider to ask for multi-level exchange of opinions between the supervisory authorities and the Crypto-Asset Exchange Service Provider. This system supervisors meaningful to help the parties share the same recognition as to the facts underlying the disposition and their severity.

In cases where, in the course of interviews, etc. in relation to the supervisory authorities' request for reporting under Article 63-15(1) of the Act, a Crypto-Asset Exchange Service Provider who was aware that an adverse disposition is likely to be rendered requested the supervisory authorities to have an opportunity of exchange of opinions between the supervisory authorities' senior officials and the executives of the Crypto-Asset Exchange Service Provider (see Notes) and when the supervisory authorities intends to render an adverse disposition which requires prior hearings or the grant of an opportunity for explanations, the supervisory authorities must provide an opportunity for exchanging opinions as to the facts underlying the intended adverse disposition and their severity. Such opinion exchange session must be held before giving a notice of hearings or notice of granting an opportunity for explanations, except where such disposition needs to be urgently rendered.

Note 1: Example of the supervisory authorities' senior officials: director of its relevant division of the FSA and the Local Finance Bureau.

Note 2: Requests by a Crypto-Asset Exchange Service Provider for an opportunity for exchange of opinions must be made during the period from the time when the supervisory authorities received a written report under Article 63-15(1) of the Act explaining the facts underlying the intended adverse disposition to the time when the supervisory authorities give a notice of

hearing or of granting an opportunity for explanation.

III-6 Ascertainment of Locations of Business Office

Where it is necessary to ascertain the location of the business office of a registered Crypto-Asset Exchange Service Provider pursuant to Article 63-17(2) of the Act, the supervisory authorities may require said Crypto-Asset Exchange Service Provider to submit a location report pertaining to the business office prepared using Appended Form 15, a document certifying the rights to the business office or a map of the business office, etc. pursuant to Article 63-15(1) of the Act. The supervisory authorities may order that such report be submitted to the Local Finance Bureau having jurisdiction over the location of such business office.

III-7 Cooperation with Relevant Authorities in Japan and Overseas Supervisory Authorities, etc.

In addition to cooperation with relevant authorities in Japan, given that Crypto-Asset transactions can easily be conducted on a cross-border basis via the Internet, there are limits to how a single country can cope with such transactions, and thus international cooperation is indispensable. In light of this, the supervisory authorities shall cooperate with not only relevant authorities in Japan but also overseas supervisory authorities and international organizations when necessary, such as by sharing information, knowledge, and experience concerning the supervision of Crypto-Assets and Crypto-Asset Exchange Service Providers on a periodic or as-needed basis.

When the supervisory authorities intends to issue an order to submit reports, an order to improve business operations, or an order for business suspension, or to render an adverse disposition of revoking the registration, it shall contact the relevant authorities in Japan and overseas supervisory authorities, etc. as necessary.

III-8 Basic Stance for Public Disclosure of Adverse Dispositions

(1) When making public notice of adverse disposition pursuant to Article 63-19 of the Act, the supervisory authorities shall disclose the following particular in the public notice.
   (i) Trade name
   (ii) Name of the representative
   (iii) Location of the headquarters
   (iv) Registration No.
   (v) Date of registration
   (vi) Date of the disposition
   (vii) Details of the disposition

(2) It should be noted that the handling of public notice other than (1) above is based on the approach specified in “I-5 Transparency” of the “Principles of Financial Supervision and Instructions for Supervisory Department Staff (Code of Conduct)”.
   That is, with regard to the adverse dispositions such as orders to improve business operation, etc., the facts underlying the invocation of those dispositions, the content of dispositions, and other information shall be made public from the viewpoint of enhancing the predictability for other Crypto-Asset Exchange Service Providers and preventing recurrence of similar incidents or problems, except where the disclosure of relevant facts and information is likely to impede the business improvement efforts of the Crypto-Asset Exchange Service Provider concerned.

III-9 Notification of Administrative Disposition

(1) In the case of refusal of registration (Article 63-5 of the Act)

When refusing the registration, the Director-General of the Local Finance Bureau shall notify the Director-General of the Supervisory Bureau of the FSA to that effect by sending a written notification of refusal of registration of Crypto-Asset Exchange Service Provider using Appended Form 6 together with a copy of the written application for registration.

(2) In the case of order to improve business operation (Article 63-16 of the Act)

When issuing an order to improve business operations, the Director-General of the Local Finance Bureau shall send relevant materials to the department in charge at the FSA and the Directors-General of Local Finance Bureaus having jurisdiction over the location of the business office pertaining to the business operation of said Crypto-Asset Exchange Service Provider.

(3) In the case of an order to suspend business (Article 63-17(1) of the Act)

When issuing an order for business suspension, the Director-General of the Local Finance Bureau shall send relevant materials to the department in charge at the FSA and the Directors-General of Local Finance Bureaus having jurisdiction over the location of the business office pertaining to the business operation of said Crypto-Asset Exchange Service Provider.

(4) In the case of a disposition to revoke registration (Article 63-17 of the Act)

When revoking the registration of a Crypto-Asset Exchange Service Provider, the Director-General of the Local Finance Bureau shall send relevant materials to the divisions in charge at the FSA and other Local Finance Bureaus. In addition to the above, the Director-General of the Local Finance Bureau shall also send materials concerning the names of the officers of the Crypto-Asset Exchange Service Provider within 30 days prior to the rescission.